DOS-TREND EXTRA · Lfr 180,– · öS 62,– · sFr 8,50 · DM 8,50

DOS TREND Public Domain & Shareware

EXTRA

THUNDERBYTE ANTI-VIREN-PAKET

Sensationspreis!

DM 8,50
sFr
öS 62,–
inkl. 5¼"-Diskette!

3½"-Disk gratis anfordern!

Virengeprüft durch Thunder BYTE

Virenschutz komplett!
String-Erkennung!
Heuristische Analyse!
Integritäts-Check!

PEARL AGENCY
PD/SHAREWARE
EH002
DOS-TREND EXTRAHEFT 2
THUNDERBYTE ANTI-VIREN-PAKET
INT-NR: 200793RL27 RL000010/000005

TB-SCAN: Kein Platz für Viren

TB-MEM: Speicherüberwachung

TB-CLEAN: Eine saubere Sache

TB-FILE: Virenblocker

Treten Sie ein!

Die Windows Informations-Elite erwartet Sie bereits:

win

PC WELT

WINDOWS

WinDOS

CompuServe

Computer Solutions

G.I.B.

Willkommen im Club der WINsider

Sonderaktion

Jedes neue Mitglied erhält einmalig:

1. Ein dreimonatiges **CD-ROM** Probeabo mit drei mal 50 Windows-Programmen im Wert von **DM 29,97**.

2. Ein Expl. des HD-Disk-Sonderheftes „Windows" im Wert von **DM 15,90**.

3. Eine Ausgabe von **DOS-TREND**, dem aktuellen PC-Magazin mit Heft-Diskette im Wert von **DM 8,90**

Eintrittskarte für den W.I.S. Club

Ja, ich möchte für 12 Monate (ab Rechnungsdatum) an dem W.I.S.-Service (1–5) teilnehmen und erhalte:

1. Jährlich wahlweise 12 Ausgaben eines der folgenden Magazine (nur eine Ankreuzung ist zulässig): ☐ WIN ☐ PC-WELT ☐ WINDOWS ☐ WinDOS
2. Eine **Einführungs-Mitgliedschaft** bei **Compuserve**
3. Jährlich **12 Windows Shareware-Disketten** (360 KB)
4. Jede Ausgabe der **Windows Börse direkt**
5. Modem-Zugriff auf die **W.I.S. Online-Datenbank** und die Möglichkeit, **Produkt-Recherchen** durchzuführen.

Dafür bezahle ich 12 x DM 19,90 = 238,80 zzgl. DM 5,- Versandkostenanteil = **DM 243,80** (Auslandspreis: DM 79,50). Falls ich nicht 8 Wochen vor Ablauf schriftlich kündige, verlängert sich die Teilnahme automatisch um weitere 12 Monate.

Ich wünsche folgende Zahlungsweise (wie angekreuzt):

☐ mit beiliegendem Verrechnungsscheck

☐ gegen Rechnung

Datum/Unterschrift

✗

Name

Firma

Straße

PLZ/Ort

Tel./Fax

Widerrufsrecht: Diese Vereinbarung kann ich innerhalb von einer Woche bei G.I.B. Verlag GmbH, Albert-Schweitzer-Str. 66/EG, 8000 München 83 widerrufen. Ich bestätige die Kenntnisnahme durch meine zweite Unterschrift.

Datum/Unterschrift

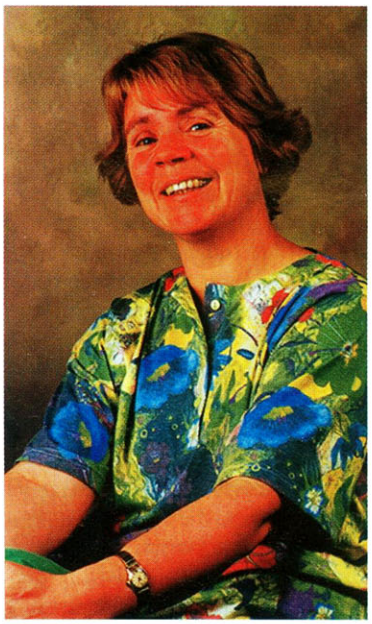
✗

PC-Welt 6/93

Eintrittskarte einsenden an:
G.I.B. Verlag GmbH, Albert-Schweitzer-Str. 66, 8000 München 83,
Telefon: (0 89) 637 03 81, **Fax: (0 89) 637 03 99**

Kennziffer 103

Es geschieht am hellichten Tage



Erinnern Sie sich noch an die Horrormeldungen, liebe Leserin, lieber Leser, als vor einigen Jahren alle Welt gebannt auf jenen berüchtigten „schwarzen Freitag" wartete, an dem der gefürchtete Israel-Virus sein unheilvolles Werk verrichten wollte? Oder an den Schrecken, der durch „Michelangelo" verbreitet wurde, der, ebenfalls an einem Freitag, dem 13., PCs und Computernetze bedrohte?

Nun, die allgemein befürchtete Katastrophe ist seinerzeit – gottlob – nicht eingetroffen. Dank der Abwehrmaßnahmen, die getroffen wurden, war es möglich, den Schaden in Grenzen zu halten. Doch das ist, leider, noch kein Grund für eine allgemeine Entwarnung. Im Gegenteil – die Gefahr, die von den programmierten Datenkillern ausgeht, ist keinesfalls gebannt, sondern wächst beständig weiter.

Begonnen hat die Geschichte der Computerviren vergleichsweise harmlos mit einem Spiel: In diesem Computerspiel mit dem Namen „Krieg der Kerne" bekämpfen sich zwei Programme, die die Fähigkeit besitzen, sich selbst zu reproduzieren; und Sieger in diesem Kampf ist das Programm, das sich selbst am stärksten zu vermehren und dabei die meisten Exemplare des Gegners zu vernichten vermag.

Was als Spiel begann und zunächst bloße Science-Fiction schien, wurde bald darauf bitterer Ernst. Seit die ersten Computerviren in den Achtziger Jahren verbreitet wurden, hat die allgemeine Plage beständig zugenommen, nicht nur in quantitativer, sondern auch in qualitativer Hinsicht. Die ungebetenen Gäste vermehren sich nicht nur geradezu epidemisch, sie haben auch dazugelernt, was die Gefährlichkeit und die Bösartigkeit angeht!

Das Thema Computerviren betrifft jeden. Kein PC-Besitzer ist gegen Virenbefall gefeit, keiner kann sich in Sicherheit wiegen. Doch deshalb besteht durchaus kein Anlaß zur Panik. Schließlich gibt es Sicherheitsvorkehrungen, und es gibt mittlerweile eine ganze Reihe von Anti-Viren-Programmen, die den Kampf gegen die gefährlichen Eindringlinge wirkungsvoll unterstützen.

Mit den Thunderbyte Anti-Viren-Utilities stellen wir Ihnen ein Virenschutzprogramm vor, das neue Maßstäbe setzt und einen bisher nicht erreichten Sicherheitsstandard bietet. Nutzen Sie den Vorteil des Sharewarekonzeptes und testen Sie das Programmpaket auf der Heftdiskette ausgiebig – sicherlich kommen auch Sie schon bald zu dem Ergebnis, daß es gegenwärtig kein wirksameres Konzept zum Schutz gegen Computerviren gibt!

Viel Spaß und eine erfolgreiche Arbeit wünscht Ihnen Ihre

Dr. Marianne Steible

Dr. Marianne Steible
DOS-TREND Redaktion

Inhalt

Vorwort 3

Einleitung 4

Installation und Programmbedienung 5

TBSETUP
Vorbeugen ist besser als heilen 6

TBSCAN
Auf Herz und Nieren 8

TBUTIL
Wehret den Anfängen 12

TBCLEAN
Keiner wäscht reiner 13

TBAV MONITOR
Kontrolle ohne Lücke 15

Kleines Bestiarium 4

Die Vollversion 18

Erste Hilfe am Unfallort 11

Einleitung

Vor einigen Jahren brachte die niederländische Firma ESaSS (Electronic Systems and Special Services) unter dem Namen „Thunderbyte" einen Virenschutz auf Hardware-Basis heraus. Dabei handelt es sich um eine PC-Einsteckkarte zur Überwachung aller Festplatten- und Speicheroperationen des Rechners.

In konsequenter Fortführung und Weiterentwicklung der Methoden und Verfahren auf dem Gebiet der Virenerkennung und Virenabwehr kann das ESaSS Entwicklungs-Team unter der Leitung des Virenexperten *Frans Veldman* nun neben der Hardware- auch die Software-Lösung präsentieren. Die Thunderbyte Anti-Viren-Utilities, abgekürzt TBAV, die wir Ihnen in diesem Heft vorstellen möchten, enthalten das komplette Instrumentarium zum Schutz vor Computerviren – von der Diagnose bis zur Prävention und zur Immunisierung. Den differenzierten Aufgaben entsprechend, baut sich das Programmpaket aus verschiedenen Teilprogrammen auf, die zum Teil aufeinander aufbauen und einander ergänzen und die in ihrem Zusammenwirken ein nahezu lückenloses Sicherheitskonzept realisieren:

TBSETUP	erstellt Prüfsummen und legt Anti-Viren-Dateien an.
TBSCAN	durchforstet Programmdateien nach bekannten und unbekannten Viren.
TBUTIL	schützt den Bootsektor und die Partitionstabelle.
TBCLEAN	entfernt auch unbekannte Viren und rekonstruiert infizierte Dateien.
TBAV-MONITOR	umfaßt alle speicherresidenten Programme: **TBSCANX** und **TBCHECK** überprüfen die Integrität von Programmdateien. **TBMEM, TBFILE** und **TBDISK** überwachen Dateien, Festplatte und Speicher.

KLEINES BESTIARIUM

Keine Angst: Mit lebendigen Viren haben Computerviren nichts zu tun. Computerviren sind Programme, die sich durch zwei markante Eigenschaften auszeichnen: Sie brauchen ein Wirtsprogramm, und sie sind in der Lage, sich zu vermehren und auszubreiten. Diesen beiden Eigenschaften oder Fähigkeiten verdankt die Spezies der Computerviren ihren Namen.

Sie verstecken sich im Code anderer Programme und tauchen deshalb auch in keinem Verzeichnis auf. Die Eindringlinge infizieren andere Programme, indem sie diese mit ihrem eigenen Programmcode überschreiben. Wird ein virulentes Programm aufgerufen, übernimmt der darin versteckte Viruscode insgeheim die Regie und kopiert seinen zerstörerischen Code in die nächste noch nicht infizierte Programmdatei. Da meist Wochen oder gar Monate vergehen, bevor der Virus aktiv wird, werden immer mehr Programme infiziert, die Verseuchung breitet sich aus, ohne daß das Verhängnis erkannt wird und Gegenmaßnahmen ergriffen werden können.

Nach ihrem Angriffsziel unterscheidet man allgemein zwei Kategorien von Computerviren: Dateiviren und Bootsektorviren.

Dateiviren: Primitive Dateiviren verbreiten sich indem sie noch nicht befallene Dateien infizieren, ohne sich jedoch im Speicher einzunisten. Residente Dateiviren dagegen setzen sich nach dem ersten Programmaufruf einer verseuchten Datei im Speicher fest und breiten sich weiter aus, indem sie weitere Dateien beim Programmaufruf infizieren. Residente Viren müssen im Speicher selbst entfernt werden, es genügt nicht, befallene Dateien zu löschen!

Eine raffinierte Abart der Dateiviren stellen die Tarnkappen- oder Stealth-Viren dar. Sie sind in der Lage, ihre Existenz zu verschleiern, indem sie bei jedem Lesezugriff auf infizierte Dateien den Originalinhalt anzeigen, so daß einige Zeit vergeht, bis die Verseuchung entdeckt wird. Ganz besonders heimtückisch und schwierig zu bekämpfen sind **polymorphe Viren**. Darunter versteht man Dateiviren, die fähig sind, sich selbst zu modifizieren und sich nach jeder Infektion neu zu verschlüsseln.

Bootsektor-Viren nisten sich im Bootsektor von Disketten oder im Master-Bootsektor der Festplatte ein und übernehmen von dort aus die Kontrolle, sowie irgendein ausführbares Programm aufgerufen wird. Je nach Angriffsziel unterscheidet man Bootsektor- und Master-Bootsektor-Viren.

Hybrid-Viren sind eine Kombination von Datei- und Bootsektorviren, die sowohl Programmdateien wie auch den Master-Bootsektor der Festplatte befallen können. Wird ein solcher Virus identifiziert, muß der Master-Bootsektor unbedingt desinfiziert werden.

Es gibt auch weitere Eindringlinge, die es in ihrer Wirkung und in ihrer Bösartigkeit durchaus mit den geschilderten Datenkillern aufnehmen können:

Trojanische Pferde sind keine Viren im engeren Sinne. Sie benötigen kein Wirtsprogramm. Sie schleichen sich in scheinbar harmloser Absicht in das System ein, um dann zur Attacke überzugehen.

Zeitbomben und **Logische Bomben** sind darauf spezialisiert, daß sie an einem bestimmten Datum oder unter einer bestimmten Bedingung hochgehen.

Auch **Dropper** sind selbst keine Viren. sondern sie schleusen Viren in Bootsektoren ein.

Das TBAV-Hauptmenü. Menüpunkte, die mit einem dreieckigen Pfeil versehen sind, öffnen ein neues Untermenü.

Programmbedienung

Bevor Sie die TBAV-Utilities installieren, sollten Sie sich eine **Sicherheitskopie der Originaldiskette** anfertigen, die Sie mit einem Schreibschutz versehen und an einem sicheren Ort aufbewahren. Um das Programmpaket auf der Festplatte zu **installieren,** wechseln Sie zu dem Laufwerk, in dem sich die Programmdiskette befindet, und geben ein:

INSTALL <Laufwerk>:\TBAV

Die Dateien werden darauf in das Verzeichnis TBAV kopiert, das bei der Installation automatisch vom Programm angelegt wird.

Nachdem Sie TBAV auf der Festplatte installiert haben, möchten Sie sich vermutlich vergewissern, ob das Programm seine Funktion auch wirklich erfüllt. Dazu muß gewährleistet sein, daß TBAV in der AUTOEXEC.BAT eingetragen ist, denn nur so können Sie sicher sein, daß TBAV seine Kontrollaufgabe bei jedem Programmaufruf wahrnimmt. Der Eintrag *once* in der **TBSTART.BAT-Datei** im TBAV-Verzeichnis, den das Installationsprogramm für Sie vornimmt, bietet darüber hinaus die Gewißheit, daß das Programm mindestens einmal täglich zur Ausführung gelangt.

Wenn Sie das **Programm** nun **starten,** erscheint sogleich der Hauptbildschirm mit dem Programmnamen und der Versionsnummer in der Titelleiste.

Das Anti-Viren-Paket TBAV besteht aus verschiedenen Einzelprogrammen, die sowohl direkt von der DOS-Kommandozeile aus wie auch über das Menü aufgerufen werden können. Wie Sie schnell feststellen werden, zeichnen sich die TBAV-Utilities durch eine moderne SAA-Oberfläche und eine übersichtliche und benutzerfreundliche Menüführung aus. Das **Hauptmenü,** das nach dem Programmstart angezeigt wird, **ist in folgende Menüs untergliedert:**

- Configure TBAV
- **TbSetup**
- **TbScan**
- **TbUtil**
- **TbClean**
- **TBAV Monitor**
- Documentation
- DEUTSCHE VOLLVERSION
- Quit and save
- Exit (no save)

Menüpunkte, die mit einem **dreieckigen Markierungszeichen** versehen sind, öffnen, wenn sie aktiviert werden, ein **neues Untermenü** mit verschiedenen Optionen, die zum Teil wiederum in Unter-Untermenüs verzweigen. Dank der streng hierarchischen Programmstruktur ist es sehr einfach, sich in den Menüs und Untermenüs zurechtzufinden, zumal die Statuszeile am unteren Bildschirmrand anzeigt, was die jeweils aktive Menüfunktion beinhaltet und bewirkt.

Die einzelnen Menüpunkte können entweder mit der **Maus** oder über die **Tastatur** durch Bewegen des Cursorbalkens mittels der Pfeiltasten oder durch Eingabe der farblich hervorgehobenen Buchstaben und der Bestätigung mit [ENTER] aufgerufen werden.

[ENTER] öffnet Menüfenster und aktiviert Programmfunktionen,

[ESC] bricht ab, schließt Fenster, führt zum übergeordneten Menü zurück und beendet das Programm.

Das ist zunächst alles, was Sie für die Programmbedienung der Thunderbyte Utilities brauchen.

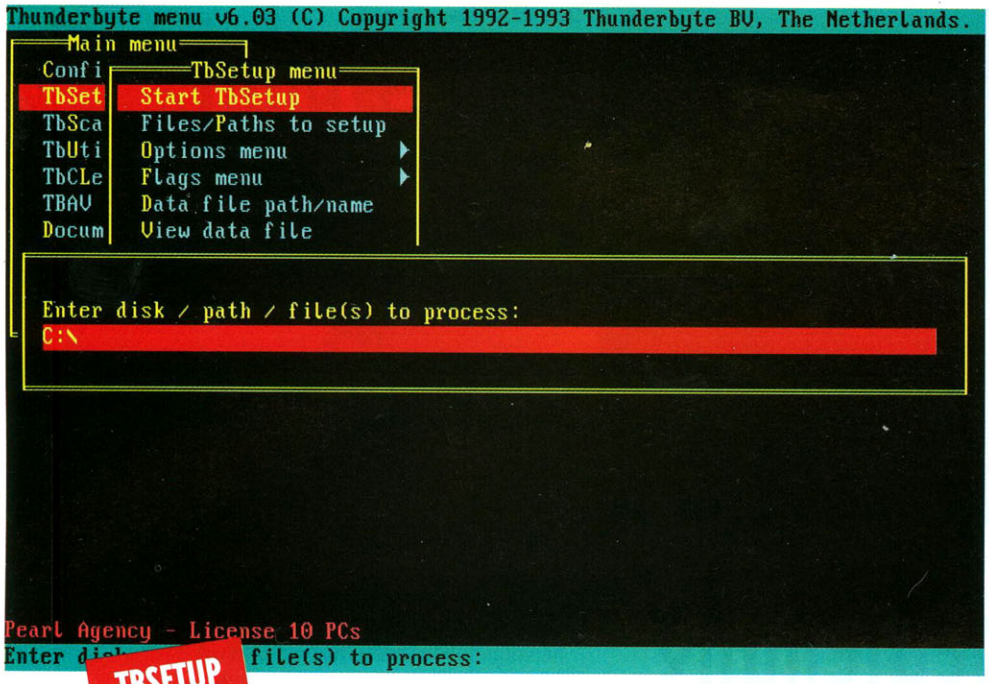
Im Bedarfsfall steht Ihnen natürlich auch eine **Online-Hilfe** zur Verfügung, die von der DOS-Kommandozeile aus aufgerufen werden kann. Kontextbezogene Hilfe erhalten Sie, wenn Sie beim DOS-Prompt den jeweiligen Programmnamen und dahinter ein Fragezeichen eingeben. Wenn Sie sich eine Übersicht über den **Inhalt der Hilfe-Datei** verschaffen wollen, so geben Sie hinter dem Programmnamen kein Fragezeichen, sondern einen Schrägstrich und *help* ein.

Um Ihnen einen schnellen Überblick zu gewähren und die Orientierung und Einarbeitung in das Programm so einfach wie möglich zu gestalten, folgen wir bei der Programmbeschreibung der Menüführung und der Menüstruktur, so wie sie sich auf dem Bildschirm darstellt.

Das Konfigurationsmenü *Configure TBAV* bedarf keiner besonderen Erläuterung, und auch auf die Menüpunkte *Documentation, DEUTSCHE VOLLVERSION, Quit and save* (das Programm verlassen und speichern) und *Exit (no save)* (das Programm verlassen, ohne zu speichern) brauchen wir nicht weiter einzugehen. Unsere Programmbeschreibung beginnt deshalb mit dem Menü TBSETUP.

Menüpunkte, die mit einem dreieckigen Markierungszeichen versehen sind, öffnen, wenn sie aktiviert werden, ein neues Untermenü mit verschiedenen Optionen, die zum Teil wiederum in Unter-Untermenüs verzweigen.

Kontextbezogene Hilfe erhalten Sie, wenn Sie beim DOS-Prompt den jeweiligen Programmnamen und dahinter ein Fragezeichen eingeben.



TBSETUP

Vorbeugen ist besser als heilen

Beim ersten Programmaufruf wählen Sie die Option *Start TbSetup.* Wenn Sie das SETUP-Programm schon einmal absolviert haben, wählen Sie die zweite Option *Files/Paths to setup.*

Sie können das SETUP-Verfahren mit [STRG] + [BREAK] abbrechen.

Das Programm **TBSETUP** läuft auf jedem Standard-PC unter dem Betriebssystem MS-DOS ab Version 3.0 und benötigt nur 140 KB freien Arbeisspeicher. TBSETUP ist selbst kein Virendetektor, sondern ein Hilfsprogramm, ein **Utility** sozusagen **für die Utilities TBSCAN, TBCHECK und TBCLEAN.** Das Programm hat die Aufgabe, Datei-Informationen zu sammeln, die im Falle einer Virusattacke benötigt werden, um den Virus zu identifizieren und die Datei in ihrem ursprünglichen Zustand zu restaurieren. Damit diese Informationen im Ernstfall unversehrt bleiben und jederzeit original zur Verfügung stehen, speichert TBSETUP die entsprechenden Daten, die mathematisch auf sogenannte **Prüfsummen** heruntergerechnet werden, in einer eigenen Anti-Viren-Datei. Diese **Anti Viren-Dateien** sind also nichts anderes als versteckte Sicherungs-Files, die in einem einmaligen Arbeitsgang – eben dem Setup-Verfahren – zu jeder Programmdatei angelegt werden. Sie stehen im selben Verzeichnis wie die Originaldatei, bleiben aber ihrem Sinn und Zweck entsprechend verborgen. Sollte es früher oder später zu einem Virenbefall und zu einer Infektion kommen, können die Informationen der Anti-Virus-Dateien genutzt werden, um den Virus zu eliminieren und die beschädigten Daten wiederherzustellen.

So viel einleitend zum Sinn und zur Aufgabe des Setup-Programms.

Das Setup-Verfahren

Wird das Setup-Programm über das Menü TBSETUP aktiviert, so öffnet sich ein neues Menüfenster mit folgenden Untermenüs:

- Start TbSetup
- Files/Paths to Setup
- Options menu
- Flags menu
- Data file path/name
- View datafile

Wenn Sie das Setup-Programm aktivieren wollen, stehen zwei Menüoptionen zur Auswahl:

- Start TbSetup
- Files/Paths to setup

Beim **ersten Programmaufruf** wählen Sie die Option *Start TbSetup* und bestätigen im folgenden Eingabefenster die voreingestellte Eingabe

C:\ mit [ENTER].

Wenn Sie das Setup-Programm schon einmal absolviert haben und das Programm zu einem späteren Zeitpunkt erneut aufrufen wollen, um Anti-Viren-Files für neu hinzugekommene Dateien anzulegen oder um bestehende Anti-Viren-Dateien zu aktualisieren, wählen Sie die **zweite Option** *Files/Paths to setup,* geben in dem Eingabefenster, das eingeblendet wird, den Namen und den Pfad der gewünschten Datei(en) ein und bestätigen Ihre Eingabe wie gewohnt mit [ENTER]. Wird außer dem Laufwerk auch der Pfad angegeben, ohne daß ein Dateiname hinzugefügt wird, so werden auch Unterverzeichnisse in das Verfahren einbezogen. Wenn jedoch ein Dateiname eingetragen wird, folgt das Programm strikt dem Pfad, ohne daß Unterverzeichnisse Berücksichtigung finden.

Beim Ablauf des Setup-Verfahrens, das übrigens jederzeit mit [STRG]+[BREAK] abgebrochen werden kann, ist der Bildschirm in **drei Fenster** unterteilt: Im **oberen Info-Fenster** lesen Sie allgemeine Programminformationen. Im **Hauptfenster** in der unteren Bildschirmhälfte links werden die Verzeichnisse und die Dateinamen angezeigt, die gerade bearbeitet werden, außerdem erhalten Sie dort alle einschlägigen Informationen, die auf mögliche Veränderungen und Manipulationen hinweisen könnten.

Im **Status-Fenster** unten rechts erfahren Sie, wieviele Verzeichnisse und Dateien insgesamt in das Setup-Verfahren einbezogen wurden, wieviele Dateien davon gesondert behandelt werden, und wieviele Anti-Viren-Dateien angelegt worden sind.

Welche Informationen werden im Hauptfenster ausgegeben?

Zunächst wird der **Dateiname**, die **Dateilänge** (hexadezimal) und die **Prüfsumme** (32 Bit CRC) angezeigt.

Weiterhin sehen Sie, was im Setup-Programm gerade abläuft. Folgende Aktionen sind möglich:

Added: Eine Anti-Viren-Datei existiert noch nicht und wird jetzt angelegt;

Changed: Eine Anti-Viren-Datei existiert, die Ausgangsdatei wurde jedoch verändert und die Information der Anti-Virus-Datei entsprechend aktualisiert;

Updated: Eine Anti-Viren-Datei existiert bereits, die Aus-

gangsdatei selbst wurde nicht verändert, das Setup-Programm aber verändert bestimmte Markierungszeichen (aufgrund entsprechender Einstellungen im Untermenü *Flags*).

Das Sternchen *, das darauf folgen kann, weist auf Dateien hin, die aufgrund besonderer Merkmale besonders behandelt werden. Und das letzte Feld schließlich ist den **Flags** oder Markierungszeichen vorbehalten. Das sind Zeichen, die vom Programm gesetzt werden, wenn verdächtige Abweichungen und Veränderungen festgestellt werden.

Die Optionen

Im Setup-Programm stehen eine Reihe verschiedener Optionen zur Verfügung, mit denen Sie **auf den Ablauf des Verfahrens Einfluß nehmen** können. Die verschiedenen Optionen können als Parameter in der DOS-Kommandozeile angegeben oder über das entsprechende Menü aufgerufen werden. Wir gehen hier den einfacheren und intuitiveren Weg über das Menü und ersparen es uns auf diese Weise, uns die Kürzel für jede einzelne Option einprägen zu müssen.

- **Use TBAV.INI file:** Standardmäßig gelten die Optionen, die vom Programm voreingestellt sind und die in der Datei TBAV.INI gespeichert werden, nur innerhalb der Menüoberfläche. Wird jedoch die standardmäßig nicht aktive *Use TBAV.INI file*-Option aktiviert, dann gelten die entsprechenden Optionen auch, wenn das Programm von der DOS-Kommandozeile aus aufgerufen wird.
- **prompt for pause:** Die Bildschirmanzeige wird fensterweise angehalten
- **only new files:** Nur neue Dateien werden berücksichtigt.

Es ist **unbedingt ratsam, diese Option zu aktivieren!** Werden nicht nur neue, sondern auch bearbeitete oder veränderte Dateien in das Setup-Verfahren einbezogen, so laufen Sie Gefahr, daß auch die Daten in der entsprechenden Anti-Viren-Datei aktualisiert und damit überschrieben werden und dann im Falle einer Vireninfektion nicht mehr zur Identifizierung herangezogen werden können!

- **Remove Anti-Vir.Dat files**: Anti-Viren-Dateien werden entfernt.
- **Do not change anything:** Das Setup-Programm nimmt keinerlei Veränderungen vor.
- **Hide Anti-Vir.Dat files:** Die Anti-Viren-Dateien bleiben unsichtbar.
- **Make executables readonly:** .EXE-Dateien werden mit Schreibschutzattribut versehen
- **Clear readonly attributes:** Schreibschutzattribute werden entfernt.
- **Sub-Directory Scan:** Auch Unterverzeichnisse werden überprüft.

Die Optionen für das Setzen von Markierungszeichen sind zusammengefaßt im *Flags menu*. Wenn Sie die vom Programm standardmäßig voreingestellten Markierungszeichen übernehmen wollen, was zu empfehlen ist, aktivieren Sie die Option *Use normal flags*. Die Optionen *Set flags manually* und *Reset flags manually* sollten **nur von sehr erfahrenen und fachkundigen Anwendern** eingesetzt werden. Nähere Informationen dazu erhalten Sie in der Dokumentation zum Setup-Menü. Die Anweisung *Define flags* bietet die Möglichkeit, Markierungszeichen zu definieren, die – abweichend vom Standardverfahren – nicht gesetzt werden sollen.

Das Menü *Data file path/name* wird aufgerufen, wenn Name und Pfad der Spezialdatei TBSETUP.DAT geändert werden soll.

Diese Spezialdatei ist nichts anderes als eine Liste von Dateien, die unter normalen Umständen Verdacht erwecken und Virenalarm auslösen würden.

- **View Data** *file:* Unter diesem Menüpunkt können alle erforderlichen Informationen über die Spezialdatei TBSETUP.DAT abgerufen werden.

```
Thunderbyte software setup v6.03 (C) Copyright 1992-1993 Thunderbyte B.V.
TBSETUP.DAT
 The TbSetup program stores checksum, validation, and cleaning information of
 programs in hidden Anti-Vir.Dat files. Several Thunderbyte Anti-Virus (TBAV)
 utilities use this information to enhance detection and removing of viruses.

 Programs that require special attention of TBAV utilities are listed in the
 TbSetup.Dat file. Send files that require special TBAV attention to our BBS
 for inclusion into this file! Current TbSetup.Dat revision: 6.00 / 04-15-93

C:\SGMXII\VOYETRA\SSCRIPT\
Filenames      |Length|32-bit CRC|Action |  Flags          Status
CDPLAY.EXE      00828B  D9858D0E                  TbSetup entries:   170
SGCOX.EXE       0034BC  AEEC8910
PLAY.EXE        003B8C  09E649A4                  Anti-Vir files:     30
DAPLAY.EXE      0029FF  9E043403
VMP.COM         0062E2  4F316DA1          0010    Directories:        41
TAPISG.COM      006D4A  6EF66D84          0010
SGFIG.EXE       008A0B  070C5676                  Total files:       489
SGCDU.SYS       00275B  F5E64A2B                  Executables:       133
SGVOL.EXE       00356E  17505516
SGZ.EXE         0128F3  F5CAC52B                  New files:          08
GMASTER.EXE     0285A4  57476A50                  Changed files:      00
WJUKE.EXE       017400  4E922E98
SS.EXE          00ABCB  ■                         Special files:      07
```

Den Ablauf des Setup-Verfahrens können Sie am Monitor verfolgen. Achten Sie vor allem auf Markierungszeichen, die vom Programm gesetzt werden und die auf Veränderungen aufmerksam machen!

Aktivieren Sie unbedingt die Option: *only new files.*

***Use normal flags* aktiviert die Standard-Optionen des Programms.**

***Set flags manually* und *Reset flags manually* sollten nur von sehr erfahrenen und fachkundigen Anwendern eingesetzt werden.**

Aktivieren Sie das Setup-Programm nur bei konkretem Anlaß – z.B. nach Installation eines neuen Programms.

TBSETUP.DAT

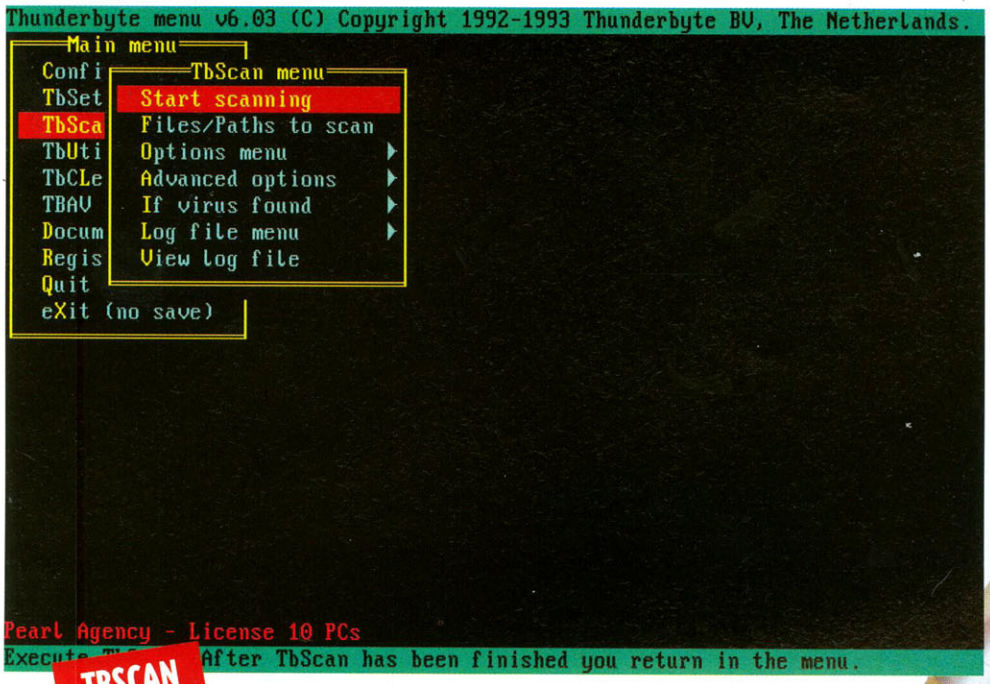
Dazu eine kurze Erklärung: Prinzipiell kann das von TBAV eingesetzte Virencheckverfahren bei allen Dateien angewandt werden. Doch es gibt Programme, die in ihrer Struktur einem Virus sehr ähnlich sind und die unweigerlich den Virenscanner TBSCAN auf den Plan rufen würden, gäbe es die **Spezialdatei** nicht, in der die Informationen und die Markierungszeichen gespeichert sind, die eine **Sonderbehandlung der betreffenden Dateien** ermöglichen und zulassen.

ANWENDER-TIPS

Das Setup-Programm sollte **auf keinen Fall unnötig und willkürlich aufgerufen** werden, sondern nur, wenn ein Anlaß dafür besteht, wenn Sie beispielsweise ein neues Programm auf Ihrem Rechner installiert haben.

Wenn das Setup-Verfahren einmal ordnungsgemäß abgelaufen ist und damit für alle Programmdateien Prüfsummen angelegt worden sind, ist es weder erforderlich noch ratsam, das Setup-Programm erneut zu starten. Der Virenschutz wird dadurch nicht erhöht – im Gegenteil!

Stellen Sie sich vor, Sie lassen das Setup-Programm erneut laufen, nachdem sich unbemerkt ein Virus in Ihr System eingeschlichen hat. Was passiert? – Sie laufen Gefahr, daß die Prüfdaten in den Anti-Viren-Files den veränderten Informationen der infizierten Dateien entsprechend aktualisiert und überschrieben werden! Das aber würde bedeuten, daß die Originaldaten der intakten Datei endgültig verloren wären und nicht mehr zur Virenerkennung und zur Restaurierung herangezogen werden könnten!



Der Virenscanner TBSCAN wird über das Menü aktiviert. Soll die ganze Festplatte überprüft werden, so wird der erste Menüpunkt *Start Scanning* aufgerufen.

TBSCAN

Auf Herz und Nieren

Soll die gesamte Festplatte gescannt werden, so bestätigen Sie TBSCAN C:

Einen wichtigen Part in den TBAV-Utilities zur Virenerkennung und Virenbekämpfung spielt der Virenscanner **TBSCAN,** den Sie nach dem Konfigurationsmenü und dem Setup-Programm an dritter Stelle im TBAV-Hauptmenü finden.

Das Programm TBSCAN läuft **auf jedem PC** und beansprucht lediglich 200 KB Speicherplatz und zusätzlich 16 KB, wenn Sie sich entschließen sollten, das optional angebotene Logfile zu benutzen. Wird das Programm über das Hauptmenü aktiviert, so erscheint das Menü TBSCAN, das verschieden Menüpunkte und Optionen anzeigt:

- Start Scanning
- Files/Paths to scan
- Options Menu
- Advanced Options
- If virus found
- Logfile menu
- View logfile

Um das Scan-Verfahren in Gang zu setzen, können Sie je nach Wunsch die erste oder die zweite Menüoption wählen. Soll die **gesamte Festplatte** gescannt werden, so bestätigen Sie

TBSCAN C:\

Wenn Sie keinen Dateinamen, sondern nur Laufwerk und Verzeichnis eingeben, werden auch die Unterverzeichnisse einbezogen. Wird dagegen ein Dateiname spezifiziert, so hält sich das Programm genau an den vorgegebenen Pfad und scannt nur die benannte Datei, ohne daß mögliche Unterverzeichnisse berücksichtigt werden.

Ähnlich wie beim Setup ist der Bildschirm auch beim Scan-Verfahren in **drei Fenster** aufgeteilt: Das **obere** Fenster ist auch hier dazu bestimmt, wichtige Informationen anzuzeigen. Entdeckt TBSCAN eine infizierte Datei, so erfolgt in diesem Fenster die entsprechende Meldung. Im **Hauptfenster** links unten können Sie verfolgen, welche Dateien gerade gescannt werden, und was dabei im einzelnen geschieht. Im **Status-Fenster** unten rechts schließlich erfahren Sie wiederum, wieviele Dateien gescannt und wieviele Viren ausfindig gemacht wurden. Außerdem wird dort angezeigt, welches File-System verwendet wird – DOS oder das programmeigene System („OWN"). TBSCAN ist nämlich in der Lage, Dateien direkt von der Festplatte zu lesen, unter Umgehung des Betriebssystems, was sowohl die **Sicherheit** wie auch die **Geschwindigkeit des Scan-Verfahrens erhöht.**

Das Hauptfenster

Schauen wir uns nun genauer an, was sich im Hauptfenster abspielt:

Das erste Feld links nimmt den Dateinamen auf. Im zweiten Feld wird das **Verfahren** beschrieben. Im folgenden Feld erscheinen die **Markierungszeichen,** die bei der **heuristischen Analyse** gesetzt werden, und im letzten Feld schließlich erfahren Sie das **Ergebnis des Prüfverfahrens.**

Die Angaben im zweiten Feld, die das laufende Verfahren beschreiben, beziehen sich auf die unterschiedlichen **Such-Algorithmen,** die je nach Datei vom Programm eingesetzt werden. Folgende Angaben sind möglich:

- looking
- checking
- tracing
- scanning
- skipping

Nähere Informationen dazu entnehmen Sie der TBSCAN-Dokumentation.

Entdeckt TBSCAN eine infizierte Datei, so wird dies umgehend gemeldet. Welche Konsequenzen Sie in einem solchen Falle ziehen können, wird weiter unten besprochen. An dieser Stelle wollen wir zunächst auf die **möglichen Meldungen** eingehen, die bei einem Virenbefall im entsprechenden Info-Fenster ausgegeben werden:

- **Infected by [xy]virus** – die Datei ist von dem in Klammern genannten Virus infiziert;

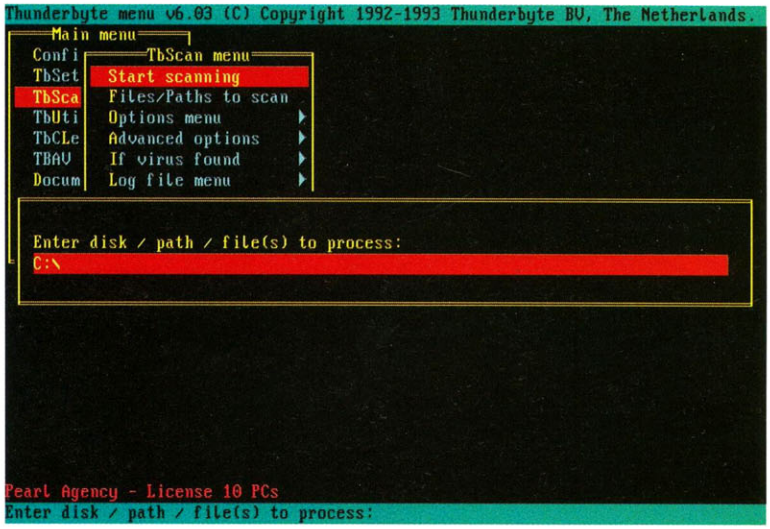
- **Dropper of [xy]virus** – die Datei ist nicht selbst infiziert, enthält aber einen Bootsektor-Virus, der sich von der Datei aus im Bootsektor einnisten könnte;
- **Damaged by [xy]virus** – die Datei ist beschädigt, enthält aber – im Unterschied zu einer infizierten Datei – den Virus nicht mehr;
- **Overwritten by [xy]virus** – die Datei wurde überschrieben;
- **Is Trojan named** – Vorsicht! Die Datei entpuppt sich als Trojanisches Pferd und sollte so schnell wie möglich gelöscht werden!
- **Is Joke named** – es handelt sich um einen Scherz, ein Virenbefall wird nur simuliert.

„Trojanische Pferde"

Trojanische Pferde vervielfältigen sich nicht. Diese Spezies zählt deshalb auch nicht zu den Viren im engeren Sinne, vielmehr handelt es sich um eine **nicht minder gefährliche Abart,** die ebenfalls nicht unterschätzt werden sollte. Wie der Name es schon verrät, schleichen sich Trojanische Pferde getarnt und in scheinbar harmloser Absicht in das System ein, um dort ihr zerstörerisches Werk zu verrichten.

In bestimmten Fällen wird vom Programm die zusätzliche Menüoption *Validate* angeboten, die einer kurzen Erklärung bedarf:

Wie Sie noch vom vorangegangenen Kapitel über das Setup-Programm wissen, gibt es **Dateien, die sich anders als normale Dateien verhalten** und für die deshalb so etwas wie **Ausnahmeregeln** gelten. Um unnötigen Fehlalarm zu vermeiden, werden bei diesen Dateien die sonst üblichen Markierungszeichen bei Veränderungen und Unregelmäßigkeiten nicht gesetzt. Wenn nun bei der heuristischen Analyse einer solchen Datei eine mögliche Infizierung entdeckt wird, so wird in dem Fenster, in dem die Virenmeldung erscheint, die Option *Validate program* angeboten. Wenn Sie sich ganz sicher sind, daß bei der betreffenden Datei kein Virus im Spiel ist, bestätigen Sie diese Option. Damit erreichen Sie, daß künftig kein Fehlalarm mehr erfolgt. Und noch ein weiterer Zusatz bei einer Virenmeldung ist möglich und soll nicht unerwähnt bleiben: Es kann vorkommen, daß TBSCAN **einen Virus vermutet,** ohne daß dieser Verdacht durch eine Signatur verifiziert werden kann. In einem solchen Falle wird der Meldung „infected" der einschränkende Hinweis „probably" (vermutlich) oder „might be" (möglicherweise) hinzugefügt.



Wenn ein bestimmtes Laufwerk oder Verzeichnis gescannt werden soll, aktivieren Sie den Menüpunkt *Files/Paths to scan* und geben den gewünschten Pfad in der entsprechenden Eingabemaske ein.

Das Optionen-Menü bietet die Möglichkeit, auf den Ablauf des Scan-Verfahrens Einfluß zu nehmen.

Optionen

Wie TBSCAN beim Scannen im einzelnen vorgeht, das hängt von den Optionen ab, die durch die entsprechenden Parameter in der DOS-Kommandozeile bzw. unter den Menüpunkten *Options Menu* und *Advanced options* im Hauptmenü des Programms aktiviert werden können.

Das *Options Menu* enthält die folgenden Anweisungen:

- **Use TBAV.INI file:** vgl. dazu die entsprechenden Erklärungen auf S. 7.

Falls TBSCAN einen Virus nur vermutet, ihn aber nicht verifizieren kann, wird der Hinweis „probably" oder „might be" gegeben.

ANWENDER-TIPS

Sie wissen jetzt, wie TBSCAN funktioniert und welche Menüpunkte und Optionen Ihnen im einzelnen zur Verfügung stehen. Nun möchten Sie sicherlich auch erfahren, wann Sie TBSCAN einsetzen und wie Sie dabei vorgehen sollten.

Einmal wöchentlich sollten Sie sich unbedingt die Zeit nehmen, TBSCAN von einer bootfähigen und schreibgeschützten Diskette aus zu starten. Nur so können Sie einigermaßen sicher sein, daß sich in Ihrem Speicher kein Tarnkappen- oder Stealth-Virus einschleicht. Falls Sie bis jetzt noch keine entsprechende **Boot-Diskette für TbScan** angefertigt haben, so sollten Sie dies jetzt tun. Gehen Sie dabei folgendermaßen vor: Booten Sie Ihren PC von Ihrer Original-DOS-Diskette aus und kopieren Sie die DOS-Diskette mit dem Befehl *diskcopy* auf eine neue Diskette. Dann löschen Sie auf dieser neuen Diskette alle Dateien, ausgenommen die beiden versteckten Systemdateien und die Datei COMMAND.COM. Dann kopieren Sie alle TBSCAN-Dateien auf die Diskette und legen eine neue AUTOEXEC.BAT an, die die Zeile

TbScan C:

enthalten sollte. Abschließend versehen Sie Ihre Boot-Diskette mit einem Schreibschutz.

Für die **tägliche Sicherheitsroutine** genügt es, wenn Sie TBSCAN ganz normal vom Verzeichnis Ihrer Festplatte aus aufrufen und in Aktion treten lassen.

Nach der Viren-Meldung wird eine Warnung eingeblendet: TBSCAN hat den Tequila-Virus ausfindig gemacht.

```
Thunderbyte virus detector v6.03 - (C) Copyright 1989-1993, Thunderbyte B.V.

                    WARNING!

B:\LHARC.EXE
 infected by Tequila (1) virus

Heuristic flags: caTG
c  No checksum / recovery information (Anti-Vir.Dat) available.
a  Found an instruction decryption routine.  This is common
   for viruses but also for some protected software.
T  Incorrect timestamp.  Some viruses use this to mark infected files.
G  Garbage instructions.  Contains code that seems to have no purpose
   other than encryption or avoiding recognition by virus scanners.

D)elete, R)ename,
C)ontinue (do nothing), N)onStop continue, Q)uit TbScan?  >

elapsed time:    00:05
Kb / second:     00
```

Die Option *extract signatures* ist nur in der registrierten Vollversion des Programms verfügbar und braucht uns hier nicht zu beschäftigen.

Mit der Option *Auto heuristic sensitivity* schaltet das Programm erst bei Verdacht auf die sensiblere Stufe 2 um.

- **Prompt for pause:** Pause nach jedem Meldefenster
- **Quick scan:** Nur Dateien mit veränderter Prüfsumme oder ohne Prüfsumme werden (mit Hilfe der Anti-Virus-Dateien) gescannt
- **Non-executable scan:** Alle Dateien werden gescannt (auch nicht-ausführbare Dateien)
- **Maximum Compatibility:** Eine maximale Kompatibilität des Programms mit dem System wird angestrebt. Das Verfahren wird damit freilich verlangsamt!
- **Bootsector scan:** Der Bootsektor wird gescannt
- **Memory scan:** Der Arbeitsspeicher wird gescannt
- **HMA scan forced:** Der HMA-Speicher wird gescannt.
- **Upper memory scan:** Auch der Speicherbereich des upper memory wird gescannt.
- **Sub-Directory scan:** Auch Unterverzeichnisse werden gescannt.
- **Repeat scanning:** Mehrere Disketten werden gescannt, ohne daß das Programm zwischendurch zum DOS-Prompt zurückkehrt.
- **Abort on Ctrl-Break:** Wenn diese Option aktiviert ist, kann das Scan-Verfahren abgebrochen werden.

Advanced Options

Für eine besonders eingehende und kritische Überprüfung Ihrer Dateien stehen Ihnen im Zusatzmenü *Advanced options* noch folgende Optionen zur Auswahl:

- High heuristic sensivity
- Auto heuristic sensivity
- Low heuristic sensivity
- Extract signatures

Die Option *extract signatures* ist **nur in der registrierten Vollversion** des Programms verfügbar und braucht uns hier nicht zu beschäftigen. Die anderen drei Optionen, die die Intensität der heuristischen Analyse betreffen, bedürfen jedoch einer kurzen Erläuterung:

Wie bereits ausgeführt, ist die heuristische Analyse darauf ausgerichtet, verdächtige Befehlssequenzen in Programmdateien aufzudecken. Grundsätzlich unterzieht TBSCAN alle Dateien, die gescannt werden, einer heuristischen Überprüfung, diese erfolgt jedoch in zwei Stufen. **Auf Stufe 1** *low heuristic sensitivity* ist die **Toleranzschwelle für eine Virenwarnung** vergleichsweise **hoch** angesetzt.

Bei Virenverdacht werden zwar die entsprechenden Markierungszeichen gesetzt, es erfolgt jedoch **keine Warnung.** Eine solche Warnung wird nur ausgegeben, wenn die heuristische Analyse auf **Stufe 2** abläuft, wenn die Option *high heuristic sensitivity* eingestellt ist. Wird dieser Option entsprechend eine **heuristische Voll-Analyse** auf Stufe 2 vorgenommen, so reagiert das Programm also sehr viel **sensibler**, als dies auf Stufe 1 der Fall ist. Was wird damit erreicht?

Die Wahrscheinlichkeit, daß ein noch nicht identifizierter Virus auf diese Weise entdeckt wird, ist sehr viel höher als beim Standard-Verfahren. Für diesen Gewinn an zusätzlicher Sicherheit muß freilich das **Risiko häufigeren Fehlalarms** in Kauf genommen werden.

Wenn Sie sich nicht sicher sind, welche Option sie einstellen sollen, ob *low heuristic sensitivity* oder *high heuristic sensitivity* vorzuziehen ist, bietet Ihnen die Option *Auto heuristic sensitivity* einen vernünftigen Ausweg. Mit dieser Option erreichen Sie, daß TBSCAN standardmäßig das low-level Verfahren auf Stufe 1 anwendet, **bei Verdacht auf einen Virus jedoch automatisch auf die high-sensitivity Stufe 2 überwechselt,** auch wenn die Option *high heuristic sensitivity* nicht aktiviert ist.

Die Markierungszeichen, die von TBSCAN gesetzt werden, können aus kleinen oder großen Buchstaben bestehen. Kleine Buchstaben haben eher geringe Bedeutung, große Buchstaben hingegen weisen auf eine ernstere Gefahr und möglicherweise auf einen Virus hin.

Was geschieht wenn ein Virus entdeckt wurde?

Auch hier stehen Ihnen verschiedene Möglichkeiten offen, die unter dem Menü *If virus found* aufgelistet sind und aktiviert werden können:

- Present action menu
- Just continue (log only)
- Delete infected file
- Rename infected file

Wenn die erste Option *Present action menu* eingestellt ist, werden Sie bei einer Virenmeldung aufgefordert, eine der im Anschluß aufgeführten Optionen oder Anweisungen zu bestätigen.

Entscheiden Sie sich für die Option *Just continue (log only)*, so geschieht nichts weiter, als daß die infizierte Datei in das Logbuch aufgenommen wird. Ein solches Logbuch wird von TBSCAN angelegt, um Informationen über infizierte Dateien dort zu sammeln.

Wenn die Option *Delete* spezifiziert ist, wird die befallene Datei gelöscht.

Ist die *Rename*-Option aktiviert, wird der erste Buchstaben in der Datei-Erweiterung durch den Buchstaben „V" ersetzt und die Datei auf diese Weise umbenannt. Damit erreichen Sie, daß das **infizierte Programm nicht mehr aufgerufen und der Virus nicht weiterverbreitet** werden kann. Das Programm wird jedoch nicht gelöscht, sondern kann gegebenenfalls von Viren befreit und repariert werden.

Das Logbuch

Wenn Sie sich entschließen, ein Logbuch zu verwenden, in dem Informationen über infizierte Dateien gesammelt werden, so steht Ihnen hierfür ein eigenes *Log-Menü* mit verschiedenen Optionen zur Verfügung. Unter dem ersten Menüpunkt *Log file path/name* können Sie Laufwerk, Verzeichnis und Namen des

Log-files festlegen. Standardmäßig legt TBSCAN die entsprechende Datei unter dem Namen TBSCAN.LOG im aktuellen Verzeichnis an. Wenn Sie die folgende Option *Output to log file* bestätigen, wird das Logbuch automatisch vom Programm erstellt. Nun brauchen Sie nur noch zu entscheiden, welche Dateien im einzelnen in das Logfile einbezogen werden sollen. Dazu rufen Sie das Untermenü *Specify log level* auf. Insgesamt stehen Ihnen **5 verschiedene Levels** zur Verfügung:

0 nur infizierte Dateien werden gelogt. Wurden keine infizierten Dateien gefunden, so wird das Logbuch nicht erstellt bzw. nicht überschrieben,

1 wie bei Level 0, zusätzlich wird ein „summary" und ein „timestamp" in die Log-Datei eingetragen,

2 jedoch auch verdächtige Dateien aufgenommen,

3 wie bei Level 2, zusätzlich werden auch Dateien einbezogen, die beim Scannen mit einem Warnzeichen versehen werden,

4 alle Dateien (auch die nicht infizierten) werden im Logfile aufgenommen.

Wünschen Sie, daß auch die heuristische Analyse bzw. die Beschreibung dieser Analyse im Logfile erscheinen soll, deaktivieren Sie die Option *No heuristic descriptions*; und wenn Sie sichergehen wollen, daß eine schon existierende Logdatei nicht überschrieben wird, dann bestätigen Sie die Anweisung *Append to existing log*.

Bleibt abschließend noch der letzte Menüpunkt *View log file* im Hauptmenü von TBSCAN zu erwähnen. Dieser Menüpunkt gibt Ihnen Gelegenheit, sich ein bestehendes Logbuch anzusehen. Je mehr Erfahrung Sie im Umgang mit den Thunderbyte-Utilities gesammelt haben, desto interessanter kann für Sie nämlich das „Blättern" im Logbuch sein.

Erste Hilfe am Unfallort

Was tun, wenn das System oder Dateien von einem Virus infiziert sind?

1. Schalten Sie den Rechner für mindestens 10 Sekunden aus! Ein Reset genügt nicht, da viele Viren einen Warmstart überleben.
2. Booten Sie den Rechner erneut von einer schreibgeschützten DOS-Diskette.
3. Starten Sie darauf TBSCAN oder einen anderen Viren-Scanner ebenfalls von einer schreibgeschützten Diskette und nicht von der Festplatte aus. Erst wenn Sie sicher sind, daß der Hauptspeicher virenfrei ist, gehen Sie daran, die Dateien auf der Festplatte zu scannen.
4. Vergessen Sie nicht, auch den Master-Bootsektor der Festplatte zu überprüfen.
5. Haben Sie den Virus aufgespürt, löschen Sie die infizierten Dateien. Oder Sie versuchen mit Hilfe von TBCLEAN, die verseuchten Dateien zu säubern und den Virus zu entfernen.
6. TBCLEAN ist kein Backup-Ersatz und auch keine Dauerlösung. Infizierte Programmdateien sollten auch nach erfolgreicher Desinfizierung nicht weiterverwendet werden. Arbeiten Sie deshalb grundsätzlich nicht mit Originaldisketten, sondern mit Sicherungskopien, und nehmen Sie sich die Zeit, die betroffenen Programmdateien mit Hilfe der Originaldisketten neu zu installieren.

WIE ARBEITET EIN VIRENSCANNER?

Scanner sind gewissermaßen die Spürhunde auf der Jagd nach Computerviren. Sie durchforsten die Bereiche, in denen Viren sich allgemein einzunisten pflegen – den **Bootsektor** und die **Programmdateien.** Worum geht es bei dieser Suche konkret?

Das Ziel besteht darin, den Programmcode des Virus zu knacken und die ungebetenen Gäste auf diese Weise dingfest zu machen. Damit nicht der gesamte Code durchkämmt werden muß, beschränken Scanner ihre Suche auf die markanten Strings oder Zeichenketten, das heißt auf die Bytesequenzen, die für den Virus typisch sind – die sogenannten Kennungen oder Signaturen.

So weit so gut. Doch die Sache hat einen Haken: Sie setzt voraus, daß der Virus bekannt ist, und sie funktioniert nur, wenn die den Virus entlarvende Zeichenkette oder Signatur im Programm des Scanners bereits eingebaut ist. Und genau das ist der **Schwachpunkt der herkömmlichen Scanner:** Fixiert auf konstante Zeichenketten und Virensignaturen, sind sie gegen Viren, die noch nicht identifiziert sind oder die sich geschickt zu tarnen oder zu modifizieren verstehen, so gut wie machtlos!

TBSCAN ist mehr als nur ein gewöhnlicher Scanner. Das Programm ist nicht nur in der Lage, mehr als 2500 Virensignaturen in bislang unerreichter Geschwindigkeit zu erkennen, **es vermag auch, neuen, noch unbekannten Viren auf die Spur zu kommen!** TBSCAN kombiniert verschiedene Methoden und Techniken in einem Programm: **Integritäts-Check, Signaturen-Scannen und „heuristische" Analyse.**

Integritäts-Check

Beim **Integritäts-Check** wird überprüft, ob auf der Festplatte irgendwelche unzulässigen Veränderungen vorgenommen wurden. Dabei werden logischerweise nur die Bereiche überprüft, die grundsätzlich nicht verändert werden sollten, also das Betriebssystem und alle Arten von Anwendungssoftware, nicht aber Ihre persönlichen Arbeitsdateien.

Um unerlaubte Manipulationen feststellen zu können, werden für alle Programmdateien auf der Festplatte Prüfsummen errechnet. Bei einer späteren Virenüberprüfung werden die Daten der Originaldatei mit den Daten der aktuell vorliegenden Datei verglichen. Ergeben sich Abweichungen, so besteht zumindest der Verdacht, daß ein Virus am Werke war, denn keine Datei bleibt bei einer Vireninfektion unverändert.

Um eine Integritätsprüfung und einen Prüfsummenvergleich vornehmen zu können, benötigt TBSCAN das Hilfsprogramm TBSETUP, das Sie im vorausgegangenen Kapitel ja schon kennengelernt haben. Sie erinnern sich sicherlich: TBSETUP legt zu jeder in Betracht kommenden Datei eine spezielle Anti-Viren-Datei an, in der die wichtigen Informationen – sprich Prüfsummen – gespeichert werden. Wird eine Datei von einem Virus infiziert, so wird sie zwangsläufig in irgendeiner Form verändert. Dadurch stimmen die in der Anti-Viren-Datei gespeicherten Informationen mit den Informationen der infizierten Ausgangsdatei nicht mehr überein. TBSCAN überprüft automatisch alle Dateien, für die eine Anti-Viren-Datei angelegt wurde, und gibt bei jeder Abweichung oder Veränderung, die entdeckt wird, eine entsprechende Meldung aus. So viel zum Integritäts-Check.

Heuristische Analyse

Was heißt „heuristisch"? Was hat man sich unter einer „heuristischen" Analyse vorzustellen?

Anders als beim herkömmlichen Scannen werden beim „heuristischen" Verfahren **keine Virensignaturen benötigt.** Die Vorgehensweise ist weniger byte- als vielmehr befehlsorientiert. Das Ziel dieses Vorgehens ist es, **verdächtige Programmbefehle aufzuspüren.** Dies wird mit Hilfe eines Disassemblers ermöglicht. Dank dieses Disassemblers ist TBSCAN in der Lage, Programmbefehle zu interpretieren, das heißt in diesem Falle: auf ihre Absicht hin zu überprüfen.

Stößt TBSCAN auf Instruktionen, die Verdacht erwecken und auf einen Virus schließen lassen – beispielsweise den Befehl, Dateien zu überschreiben oder die Festplatte neu zu formatieren – so werden vom Programm automatisch Markierungszeichen gesetzt, die auf einen möglichen Virenbefall aufmerksam machen und gegebenenfalls Alarm auslösen.

***Einmal wöchentlich* sollten Sie sich unbedingt die Zeit nehmen, TBSCAN von einer bootfähigen und schreibgeschützten Diskette aus zu starten. Für die *tägliche Sicherheitsroutine* genügt es, wenn Sie TBSCAN ganz normal vom Verzeichnis Ihrer Festplatte aus aufrufen und in Aktion treten lassen.**

Legen Sie unbedingt eine bootfähige Diskette mit TBSCAN an!

TBUTIL

Wehret den Anfängen

Mit diesem Befehl werden alle wichtigen Bootsektor-, Master-Bootsektor- und CMOS-Informationen in der TBUTIL-Datei gespeichert.

Sichern Sie unbedingt die Dateien TBUTIL.DAT und das Programm auf einer extra Diskette!

Wie Sie bereits wissen, ist eine besondere Spezies der Computerviren speziell darauf abgerichtet, die **Partitions-Tabelle** und den **Bootsektor** von Disketten und Festplatten zu infizieren. Ist ein Bootsektor-Virus in das System eingedrungen, so **liegt** der gefährliche Eindringling fortan **bereits beim Booten im Speicher auf der Lauer,** darauf bedacht, neue Programme zu verseuchen, während der Anwender nichts Böses ahnend auf das Ende des Bootvorgangs wartet.

Das Programm **TBUTIL** hat die Aufgabe, diesen besonders heimtückischen Datenkillern das Handwerk zu legen. TBUTIL speichert nicht nur alle wichtigen Daten des Bootsektor-, des Master-Bootsektor- und des CMOS-Bereichs. Im Falle eines Falles ist das **Programm auch in der Lage, einen neuen, virusresidenteren Boot- und Master-Bootsektor zur Verfügung zu stellen.** Hat ein Virus den Master-Bootsektor oder die Partitions-Tabelle der Festplatte befallen, so vermag TBUTIL den Virus zu entfernen, **ohne daß die Festplatte low-level-formatiert werden muß,** selbst wenn von der Partitions-Tabelle kein Backup existiert.

TBUTIL arbeitet mit jedem IBM-kompatiblen PC und jeder Festplatte unter DOS (Version 3.0 und höher) zusammen und beansprucht nicht mehr als 64 KB RAM.

Nach dem Aufruf von TBUTIL erscheint ein neues Menü mit folgenden Menüpunkten:

- System maintenance menu
- Immunize/clean bootsector A:
- Immunize/clean bootsector B:
- Immunize/clean partition code

Das **System maintenance menu** ist dazu da, wichtige Systeminformationen zu speichern, zu vergleichen und gegebenenfalls wiederherzustellen. Wird dieses System-Menü aktiviert, so öffnet sich noch einmal ein Untermenü, das alle Optionen beinhaltet, die im Falle einer Infizierung benötigt werden.

Zunächst muß die Datei angelegt werden, die die entsprechenden Informationen und Systemdaten aufnimmt. Dazu wählen Sie den Menüpunkt *Execute TbUtil.* Als Dateiname und Pfad ist A:\TBUTIL.DAT vorgegeben. Soll die Datei einen anderen Namen oder Pfad erhalten, so wählen Sie den folgenden Menüpunkt *Name of TbUtil data file.*

Erscheint es Ihnen sinnvoll, den Rechner zu benennen, auf den sich die Daten in der TBUTIL-Datei beziehen, so aktivieren Sie die Option *Describe this machine* und geben im folgenden Eingabefeld eine Kurzbeschreibung ein.

Ganz wichtig ist der nächste Menüpunkt *Save system configuration.* Mit diesem Befehl werden alle wichtigen **Bootsektor-, Master-Bootsektor- und CMOS-Informationen in der TBUTIL-Datei gespeichert.**

Wenn Sie sicher sein wollen, daß eine Infizierung Ihres Systems durch einen Bootsektor-Virus sofort bemerkt wird, so aktivieren Sie die folgende Option *Compare system information.*

Hat sich tatsächlich ein Bootsektor-Virus in Ihrem System eingeschlichen, so wählen Sie den Befehl *Restore system configuration,* **um Bootsektor, Partitions-Tabelle und CMOS-Bereich wiederherzustellen.**

Wollen Sie den Befehl dahingehend einschränken, daß **nur der CMOS-Speicher, die Partitions-Tabelle** oder der **Bootsektor** restauriert wird, so aktivieren Sie nach dem *Restore*-Befehl die entsprechende Zusatzoption *Process CMOS-Memory*, *Process Partition Code* oder *Process Bootsector.*

Die Immun-Funktionen

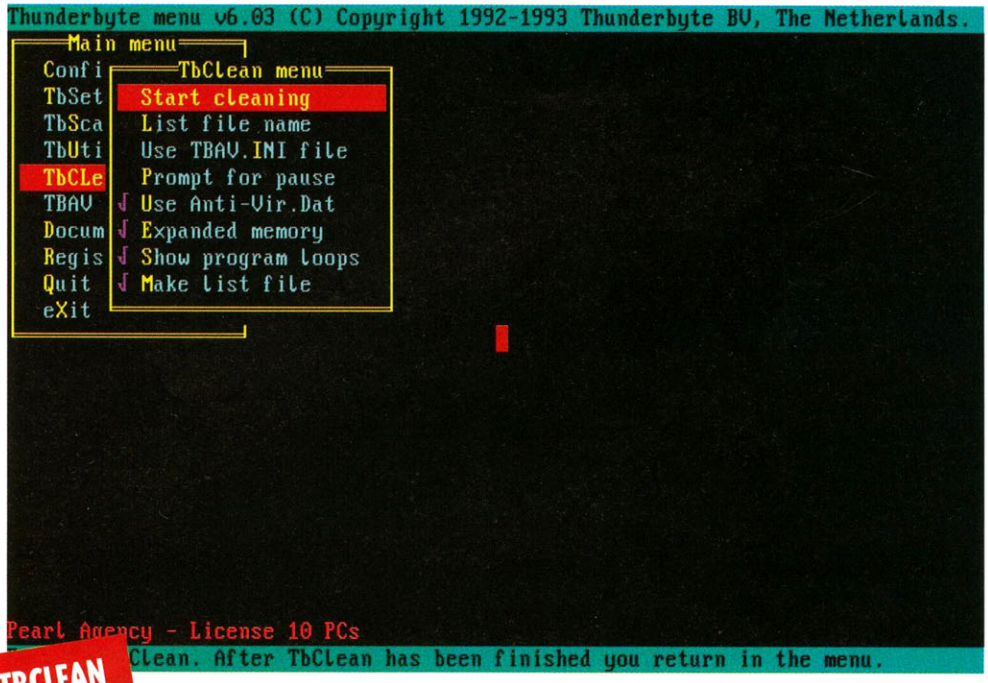
Zusätzliche Sicherheit zur Speicherung der Systemdaten gewährt die Funktion *Immunize* im Hauptmenü von TBUTIL. Je nach Bereich können Sie die Option *Immunize/clean* für den Bootsektor im Diskettenlaufwerk A oder B oder für die Partitions-Tabelle der Festplatte wählen.

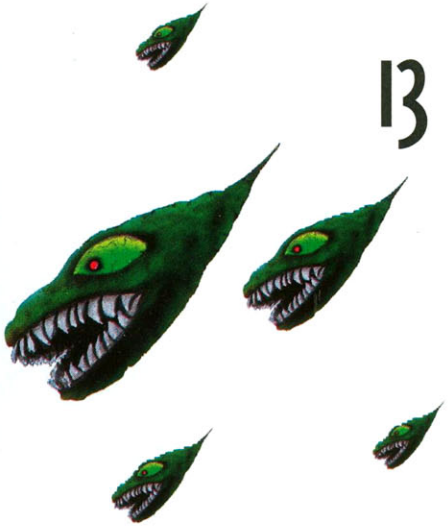
Der Befehl *Immunize/clean partition code* gibt Ihnen Gelegenheit, den **Partitions-Code der Festplatte** nach einer Infizierung durch einen Master-Bootsektor-Virus zu säubern und durch einen neuen, voll kompatiblen, aber **virus-residenteren Code** zu ersetzen. Es empfiehlt sich aber in jedem Falle, den Originalcode mit dem Befehl

TbUtil store a:tbutil.dat

auf einer Sicherungsdiskette in der Datei TBUTIL.DAT zu speichern.

Noch ein Hinweis zum Schluß: Wenn die Partitions-Tabelle von einem Virus befallen und beschädigt wurde, kann das Betriebssystem nicht mehr auf die Festplatte zugreifen, so daß Ihnen die Sicherungsdateien und Rettungsprogramme auf Ihrer Festplatte in einem solchen Falle wenig nützen. Um vorzubeugen und auf Nummer Sicher zu gehen, sollten Sie deshalb unbedingt sowohl die Datei **TBUTIL.DAT** wie das Programm **TBUTIL auf einer Diskette sichern!**





Ein Programm ist infiziert – TBCLEAN leistet Erste Hilfe! Rufen Sie das Menü auf und wählen Sie den Menüpunkt *Start cleaning*.

TBCLEAN

Keiner wäscht reiner

Wie alle Utilities im Programmpaket von TBAV läuft auch **TBCLEAN** auf jedem Standardrechner unter DOS ab Version 3.0. Das Programm benötigt mindestens 96 KB Speicherplatz. Beim **heuristischen Verfahren** ist allerdings – je nach Dateigröße – sehr viel mehr Platz erforderlich. Dabei kann **auch EMS-Speicher einbezogen** werden.

Das Menü von TBCLEAN, das keine Untermenüs beinhaltet, sondern nur einfache Befehle und Optionen enthält, wird geöffnet mit dem Befehl

Start cleaning

Wird der Start-Befehl bestätigt, so erscheint sogleich ein Eingabefeld, in dem Sie den Namen der Datei, die „gereinigt" werden soll, eingeben müssen.

Bevor die Säuberungsprozedur anläuft, wird für die entsprechende Datei ein Backup erstellt mit demselben Dateinamen, aber mit der Datei-Erweiterung .VIR.

Der **Bildschirm** beim Ablauf des CLEAN-Programms ist ähnlich aufgeteilt wie beim SETUP- und SCAN-Verfahren: Im **unteren Feld** können Sie verfolgen, was im Programm im einzelnen abläuft. In dem **blauen Balkenfeld** darüber erscheint der Name der Datei, die gesäubert und desinfiziert wird, und im **oberen Teil** des Bildschirms werden Status-Informationen ausgegeben: Im Fenster rechts werden der *entry point* (Eintrittspunkt, Startadresse), die Dateilänge und die Prüfsumme der Datei im Originalzustand, im Fenster links die entsprechenden Daten im infizierten Zustand eingeblendet.

Während des Verfahrens werden im oberen Feld über dem Dateinamen Meldungen ausgegeben, die sich auf das laufende Verfahren beziehen – zum Beispiel:

- **„Starting clean attempt. Analyzing infected file ..."** – TBCLEAN analysiert die infizierte Datei und sucht die Aufzeichnungen in der Anti-Viren-Datei – oder:
- **„Anti-Vir.Dat record found: reconstructing original state..."** – Die Aufzeichnungen in der entsprechenden Anti-Viren-Datei wurden gefunden und werden vom Programm benutzt, um die infizierte Datei zu rekonstruieren.

Aus Platzgründen ist es nicht möglich, jede einzelne Meldung, die vom Programm ausgegeben werden kann, zu übersetzen und zu erläutern. Wer sich eingehender informieren will, dem sei die Dokumentation empfohlen.

Wie alle Utilities im TBAV-Paket stellt auch TBCLEAN eine Reihe von Optionen zur Verfügung, die im

Vorbeugen ist besser als heilen! Pflegen Sie ein gut durchdachtes Backup, so daß selbst bei Virenbefall keine Daten verloren gehen. TBCLEAN ist nur ein Nothelfer, keine Dauerlösung!

ANWENDER-TIPS

Das Programm TBCLEAN ist kein Backup-Ersatz und auch kein Alibi für entsprechende Unterlassungssünden! Die gewissenhafte Anfertigung von **Sicherungskopien** ist noch immer die **wirkungsvollste Präventivmaßnahme,** um den möglichen Datenverlust bei einer Vireninfektion in Grenzen zu halten.

Fertigen Sie von jeder Originaldiskette eine Sicherungskopie an und arbeiten Sie grundsätzlich nur mit der Kopie und nie mit dem Original, das sie schreibgeschützt an einem sicheren Ort aufbewahren. Und wenn der Fall eintritt, daß ein Virus Ihr System infiziert hat, dann betrachten Sie **TBCLEAN** wie auch jedes andere Säuberungsprogramm als **Nothelfer und Rettungsanker für den Augenblick,** nicht aber als Dauerlösung. Aufgeschoben heißt nicht aufgehoben.

Nutzen Sie deshalb die nächste freie Stunde, um die betroffenen Programmdateien mit Hilfe der schreibgeschützten Originaldiskette neu zu installieren. Auf keinen Fall aber sollten Sie ein gesäubertes Programm weiter verwenden!

Wenn TBCLEAN aktiviert ist, wird ein Fenster eingeblendet, in dem alle wichtigen Informationen über die Datei, die gesäubert wird, angezeigt werden.

```
Thunderbyte clean utility v6.03 (C) Copyright 1992-1993 Thunderbyte B.V.
Infected state                          Original state
Entry point (CS:IP)                     Entry point (CS:IP)     UNKNOWN!
File length                             File length             UNKNOWN!
Cryptographic CRC                       Cryptographic CRC       UNKNOWN!

Starting clean attempt. Analyzing infected file...
C:\UIH
Pearl Agency - License 10 PCs

Can not read: C:\UIH.VIR

Press any key to return to the TBAV menu...
```

Menü angezeigt sind und die Sie zum Teil bereits kennen.

- **List file name:** Diese Option bezieht sich auf den folgenden Menüpunkt
- **Make list file:** Da dieser Menüpunkt nur für registrierte Anwender verfügbar ist, verzichten wir auf eine Erklärung.
- **Use TBAV.INI file:** Diese Option ist bereits bekannt.
- **Prompt for pause:** Auch diese Option kennen Sie schon.
- **Use Anti-Vir.Dat:** Wenn dieser Befehl deaktiviert wird, setzt TBCLEAN nur das heuristische Verfahren ein.
- **Expanded memory:** Dese Option ermöglicht es dem Programm, den EMS-Speicher zu nutzen, was die Arbeitsgeschwindigkeit erhöht.
- **Show program loops:** Wird diese Option aktiviert, so werden alle Programm-Schleifen auf dem Bildschirm angezeigt.

Vorsicht! Der Programmablauf von TBCLEAN wird damit enorm gebremst. Diese Option ist in der Regel nur für sehr erfahrene Anwender die über Programmierkenntnissen verfügen.

Verwenden Sie diese Option also nur, wenn Sie diese Information auch benötigen und interpretieren können.

Gegen die sogenannten überschreibenden Viren kann TBCLEAN nichts ausrichten. Allerdings auch kein anderes Anti-Viren-Programm!

TBCLEAN hilft Ihnen Zeit (und Geld) sparen: Es macht bei Virenbefall eine Neuformatierung Ihrer Platte überflüssig.

DAS ENTFERNEN VON VIREN: REPAIR UND HEURISTISCH

Stellen Sie sich vor, Sie entdecken, daß Sie sich einen Virus eingefangen haben, und daß eine ganze Reihe von Dateien auf Ihrer Festplatte verseucht sind. Was nun? Der Virus wurde dingfest gemacht und identifiziert, schön und gut, was aber unternehmen Sie, um den Schädling wieder loszuwerden und den Schaden zu reparieren? Die Platte putzen und neu formatieren? Alle Programme neu installieren? Das ist ganz ohne Zweifel die sicherste und zuverlässigste Lösung. Doch diese Lösung ist mühsam und kostet viel Zeit. Ganz abgesehen davon, daß Ihr Rechner bei einer solchen Aktion vermutlich für Stunden blockiert wäre und wichtige Arbeiten liegenbleiben müßten! Als Nothelfer in einer solchen Situation steht Ihnen das Säuberungsprogramm **TBCLEAN** zur Verfügung. TBCLEAN hat die Aufgabe, infizierte Dateien so weit zu säubern, daß sie nach der Desinfektion wieder normal gestartet und aktiviert werden können, ohne daß Sie Gefahr laufen, daß es zu einer neuen Infektion kommt. Wie geht diese Säuberungsaktion vonstatten? Je nach Situation setzt TBCLEAN entweder das **Repair-Verfahren** oder die **heuristische Methode** ein.

Repair-Verfahren

Das **Repair-Verfahren** basiert auf den vom SETUP-Programm generierten Anti-Viren-Dateien. Wie Sie noch wissen, werden in diesen Sicherungsdateien die Informationen gespeichert, die benötigt werden, um verdächtige Veränderungen und Manipulationen aufzudecken. Mit Hilfe dieser Informationen wie z.B. der ursprünglichen Dateilänge und der kryptographischen Prüfsumme ist es **möglich, jeden Virus aufzuspüren, egal ob bekannt oder noch unbekannt.** Um die befallene Datei zu desinfizieren, brauchen die entsprechenden Daten nur mit Hilfe der Prüfsumme verglichen und anschließend die Originaldaten wiederhergestellt zu werden, und der Schaden ist behoben.

Heuristisches Verfahren

So weit so gut. Was aber, wenn es zu einer Infektion kommt, bevor das SETUP-Programm abgelaufen ist und die erforderlichen Daten in einer Anti-Virus-Datei gespeichert wurden? Keine Sorge, auch dann ist nicht alles verloren. In einem solchen Falle springt das **heuristische Verfahren** in die Bresche. Die heuristische Analyse beim Scannen – Sie erinnern sich – ist darauf angelegt, Programmbefehle zu interpretieren und auf diese Weise die Spreu vom Weizen zu trennen, sprich: Virus-Programme von normalen Programmen zu unterscheiden. In Analogie dazu **besteht das heuristische Verfahren bei der Virenentfernung darin, den Virus in gewisser Hinsicht zu imitieren,** um ihn – wenn man so will – mit den eigenen Waffen zu schlagen!

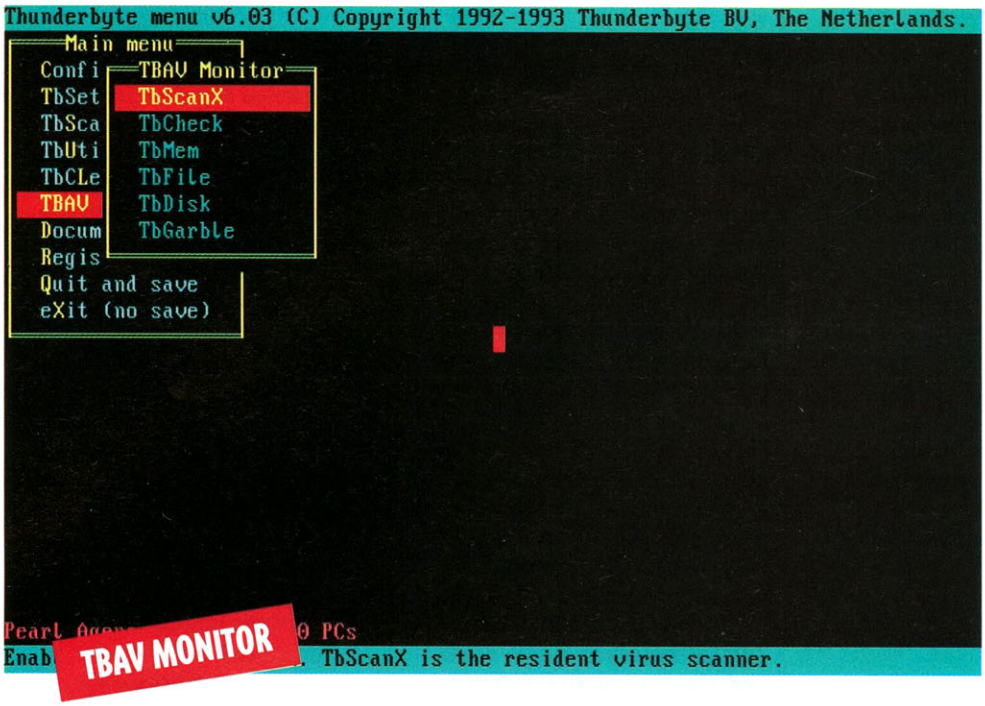
Was tut ein Virus, um andere Programme zu infizieren? Er schleicht sich in einem Wirtsprogramm ein und hängt seinen Programm-Code an den Programm-Code des Wirtsprogramms an. Um die böse Absicht in die Tat umsetzen zu können, überschreibt der Virus die ersten Bytes des Wirtsprogramms mit einem sogenannten *jump-Befehl* (jump = Sprung), übernimmt damit, wenn das Programm aufgerufen wird, selbst die Kontrolle und gibt diese Kontrolle zum Schluß wieder an das Programm zurück. Da die ersten Bytes des Programms jedoch, wie geschildert, mit dem *jump-Befehl* überschrieben wurden, muß der Virus selbst diese Bytes wieder reparieren, damit das Programm überhaupt gestartet werden kann. Und genau das ist der Schwachpunkt, den TBCLEAN beim heuristischen Verfahren zu nutzen versteht, um zerstörte Daten zu restaurieren.

TBCLEAN emuliert den Programm-Code des Virus bis zu dem Punkt, wo der Virus die überschriebenen Originaldaten wieder repariert hat und zum Originalcode zurückspringt. Darauf verabschiedet sich TBCLEAN von dem überlisteten Eindringling, kopiert den reparierten Programmanfang in die Programmdatei auf der Festplatte und entfernt den Programmteil, der die Ausführung (des Virus) beinhaltet. Auf diese Weise sind die zerstörten Daten wiederhergestellt, und der Virus ist eliminiert!

Wenn Anti-Viren-Dateien samt Prüfsummen zur Verfügung stehen und damit das Repair-Verfahren eingesetzt werden kann, **vermag TBCLEAN etwa 95% aller Viren unschädlich zu machen.** Doch selbst wenn das Programm auf das heuristische Verfahren beschränkt bleibt, weil keine Anti-Viren-Datein bestehen, sind dies immer noch um die 80%! Die einzige Viren-Gattung, bei der TBCLEAN nichts auszurichten vermag, ist die Gattung der überschreibenden Viren.

Diese Viren zeichnen sich dadurch aus, daß sie ihren Code nicht einfach an das Wirtsprogramm anhängen, sondern den Code des Wirtsprogramms **überschreiben**, der damit unrettbar verloren ist und nicht mehr rekonstruiert werden kann.

Bei so gut wie allen anderen bekannten und unbekannten Computerviren verspricht der Einsatz des Programms Erfolg. Auch die besonders heimtückischen **polymorphen Viren werden** von TBCLEAN mühelos überlistet, und selbst die gefürchtete **Mutation Engine** ist für TBCLEAN kein Problem!



TBSCANX wird speicherresident geladen und kontrolliert vom Speicher aus alle Programme, die auf die Festplatte kopiert werden.

TBAV MONITOR

Kontrolle ohne Lücke

Um eine **lückenlose Systemüberwachung** zu gewährleisten, bietet TBAV außer den bereits besprochenen Programmen TBSCAN, TBUTIL und TBCLEAN auch noch eine Reihe von **Utilities,** die dadurch charakterisiert sind, daß sie sich nach dem ersten Aufruf automatisch resident im Speicher installieren. Diese speicherresidenten Programme sind im Menü **TBAV MONITOR** zusammengefaßt und können dort aktiviert oder deaktiviert werden, vorausgesetzt, sie sind in der AUTOEXEC.BAT oder in der Batchdatei TBSTART.BAT eingetragen. Menüpunkte, die im Menü von TBAV MONITOR in blasserer Schrift erscheinen, müssen erst noch in die AUTOEXEC.BAT- oder in die TBSTART.BAT-Datei aufgenommen werden, bevor sie aufgerufen werden können. Beachten Sie bitte auch, daß die einzelnen **Monitor-Programme nur gestartet werden können, wenn das Treiberprogramm TbDriver geladen ist.**

WINDOWS-Anwender Achtung! Aktivieren Sie die residenten Monitor-Programme grundsätzlich, **bevor** Sie WINDOWS starten. Das jeweilige Monitor-Programm registriert den Aufruf von WINDOWS und schaltet sich bei Bedarf automatisch in den Multitasking-Modus von WINDOWS ein.

Das TBAV MONITOR-Menü besteht aus folgenden Programmen:

- TBSCANX
- TBCHECK
- TBMEM
- TBFILE
- TBDISK
- TBGARBLE

TBSCANX

Viren-Scanner haben normalerweise eine Achillesferse: Auch der zuverlässigste und gewiefteste Scanner kann seine Wirksamkeit nur entfalten, wenn er aktiviert ist. Worin besteht die Problematik?

Angenommen, Ihr Scanner ist in die AUTOEXEC.BAT eingetragen und tritt beim Systemstart automatisch in Aktion. Nachdem keine verdächtigen Veränderungen festgestellt wurden und keine Virenmeldung erfolgt ist, gehen Sie beruhigt an Ihre Arbeit.

Doch nun wollen Sie ein **neues Programm installieren** und die entsprechenden Programmdateien auf die Festplatte übertragen. Um sicher zu gehen, daß beim Kopieren kein Virus eingeschleust werden kann, müßte bei jeder Diskette, die auf die Festplatte kopiert werden soll, zugleich auch der Scanner gestartet werden. Und genau das ist der Schwachpunkt: Wer denkt schon daran, bei jeder Datei, die kopiert und entpackt wird, erneut den Scanner aufzurufen!

Das Problem ist nur zu lösen, wenn der **Virenscanner resident im Speicher** agiert. Und genau das ist die Aufgabe von TBSCANX. Nachdem dieser **residente Virenjäger** einmal aktiviert wurde, **bleibt** er **im Speicher und kontrolliert von dort aus alle Dateien, die Sie sich von Disketten auf die Festplatte kopieren.** Und nicht nur das: TBSCANX bietet zugleich auch **Schutz vor** den gefürchteten **Bootsektor-Viren.** Jedesmal, wenn Sie eine Diskette in Ihr Diskettenlaufwerk einlegen und starten, wird automatisch der Bootsektor überprüft.

Nachdem TBSCANX aufgerufen wurde, läuft das Programm weitgehend **unbemerkt im Hintergrund ab.** Daß TBSCANX aktiv ist, bemerken Sie erst, wenn ein Programm geladen wird oder wenn ein Schreibzugriff auf eine Datei erfolgt. In diesem Falle wird in der Ecke oben links auf dem Monitor die Meldung

Scanning

eingeblendet. Bemerkt das Programm einen unerlaubten Schreibzugriff, so erscheint ein Fenster mit der Meldung:

WARNING, <Datei> contains <virus>. Abort? (y/n) (Warnung, die Datei xy enthält den xy-Virus. Abbrechen?)

Entdeckt TBSCANX eine Virensi-

Menüpunkte, die im Menü von TBAV MONITOR in blasserer Schrift erscheinen, müssen erst noch in die AUTOEXEC.BAT- oder in die TBSTART.BAT-Datei aufgenommen werden, bevor sie aufgerufen werden können.

Beachten Sie bitte, daß die einzelnen Monitor-Programme nur gestartet werden können, wenn das Treiberprogramm TbDriver geladen ist.

WINDOWS-Anwender Achtung! Aktivieren Sie die residenten Monitor-Programme grundsätzlich, *bevor* Sie WINDOWS starten.

gnatur in einem Bootsektor, so wird ebenfalls eine Warnung ausgegeben:

WARNING, Disk in <drive> contains <virus>! Press a key
(Warnung, die Diskette in Laufwerk .. enthält den xy-Virus! Drücken Sie irgendeine Taste).

Wenn TBSCANX eine Virensignatur in einem Bootsektor entdeckt, muß die kontaminierte Diskette unbedingt aus dem Laufwerk entfernt und der Rechner neu gebootet werden!

Beachten Sie bitte, daß ein möglicher Virus zu diesem Zeitpunkt noch kein Unheil anrichten kann, da das Programm, in das der Virus sich eingenistet hat, noch nicht ausgeführt wurde. Wenn Sie jedoch die kontaminierte Diskette nicht aus dem Diskettenlaufwerk herausnehmen und den Rechner erneut booten, wird der Virus von der Diskette auf die Festplatte kopiert, und das Verhängnis nimmt seinen Lauf!

TBCHECK

Zusätzlich zum residenten Signaturen-Scanner TBSCANX bietet TBAV auch das speicherresidente Prüfsummenprogramm TBCHECK. Es hat die Aufgabe, **verdächtige Veränderungen aufzudecken,** bevor ein Programm ausgeführt wird, und bevor im Falle einer Infizierung der Virus Zerstörungen anrichten kann!

Wie können solche Veränderungen festgestellt werden? TBCHECK ist bei der entsprechenden Integritätsprüfung auf die Informationen der Anti-Viren-Dateien angewiesen. Sie erinnern sich: Die Anti-Viren-Dateien werden vom Setup-Programm generiert, um wichtige Dateiinformationen wie die Dateigröße und die Prüfsumme zu speichern. TBCHECK nutzt diese Aufzeichnungen, um verdächtige Veränderungen, die auf einen Virus hinweisen könnten, aufzuspüren.

Wie TBSCANX bleibt auch TBCHECK nach dem ersten Programmaufruf fortan **resident im Speicher,** so daß jedes Programm, das gestartet wird, sogleich auf seine Integrität hin überprüft werden kann.

Zum Programmablauf ist nicht viel zu sagen. Sichtbar tritt TBCHECK erst in Aktion, wenn ein Schreibzugriff auf eine Datei festgestellt wird – dann wird auf dem Bildschirm oben links die Meldung

Checking

eingeblendet. Im Falle, daß bei der Überprüfung eine Veränderung entdeckt wird, erfolgt augenblicklich eine entsprechende Meldung.

Wenn TBMEM resident geladen ist, können Sie bei verdächtigen Programmreaktionen das Programm selbst abbrechen, wenn es hängen bleibt: Drücken Sie einfach [STRG]+[ALT]+[EINFG].

TBMEM

Viele Viren haben die unangenehme Eigenschaft, resident im Speicher zu bleiben, nachdem es ihnen gelungen ist, sich in einem Wirtsprogramm einzuquartieren und mit Hilfe des Wirtsprogramms ihren eigenen, unheilvollen Programmcode auszuführen. Hat ein Virus sich erst einmal im Speicher eingenistet, kann er von dort aus bequem weiter agieren und andere Programme verseuchen.

Ein wirksamer Schutz gegen derartige Eindringlinge ist nur dann möglich, wenn es gelingt, **den Virus daran zu hindern, sich resident im Speicher festzusetzen.** Genau das ist die Aufgabe von TBMEM. Wie die anderen Monitor-Programme bleibt auch der Speicherwächter TBMEM nach dem ersten Programmaufruf resident im Speicher und wacht mit Argusaugen darüber, daß kein Programm nach Programmabschluß unerlaubt weiter im Speicher verweilt.

Doch wie unterscheidet TBMEM zwischen einem Virus und einem normalen TSR-Programm, das sozusagen legal im Speicher residiert? Auch TBMEM ist dazu wie schon TBCHECK auf die Unterstützung des Setup-Programms und der Anti-Viren-Dateien angewiesen. Normale TSR-Programme, die erlaubtermaßen im Speicher weilen, erhalten beim Setup-Verfahren ein entsprechendes Markierungszeichen und werden darauf von TBMEM entsprechend gesondert behandelt.

Wenn TBMEM ein Programm ausfindig macht, das sich im Speicher festzusetzen versucht, erscheint ein Fenster mit einer entsprechenden Meldung, und Sie werden vor die Alternative gestellt, dies zu verhindern oder zu gestatten. Entscheiden Sie sich nach eingehender Prüfung, das Programm fortzuführen, so setzt TBMEM in der dazugehörigen Anti-Viren-Datei automatisch ein Markierungszeichen, so daß beim nächsten Programmaufruf keine störende Meldung mehr erfolgt.

Wenn Ihnen das Verhalten des betreffenden Programms jedoch unzulässig oder auch nur verdächtig erscheint, so ist es ratsam, das Programm zu beenden und Ihren Scanner aufzurufen. TBMEM stellt Ihnen für diesen Fall die Tastenkombination [STRG]+[ALT]+[EINFG] als speziellen Hotkey zur Verfügung, mit dem das Programm jederzeit abgebrochen werden kann, auch wenn es hängen sollte!

TBFILE

Dateiviren sind darauf ausgerichtet, Programmdateien zu infizieren. Dabei führt jede Infizierung unweigerlich zu Modifikationen, egal, was der Virus im einzelnen treibt. Um eine Infizierung aufzudecken und einen Virus zu überführen, ist es unerläßlich, **das System ständig auf verdächtige Dateiveränderungen hin zu überwachen.** Diese Aufgabe übernimmt TBFILE. Das speicherresidente Überwachungsprogramm paßt auf, daß kein Programm ein anderes infiziert, und schlägt Alarm, wenn verdächtige Manipulationen beobachtet werden.

Um eine Datei infizieren zu können, muß das read-only-Attribut erst entfernt werden. Ein solches Unterfangen ist in jedem Falle virenverdächtig!

Natürlich ist nicht jede Dateiveränderung auf einen Virus zurückzuführen. Wenn ein Programm nur neu konfiguriert oder upgedatet wird, dann handelt es sich um durchaus legitime Manipulationen, die selbstverständlich keinen Virenalarm auslösen sollen. TBFILE ist in der Lage, zulässige und unzulässige Manipulationen zu unterscheiden, so daß Sie nicht mit allzu häufigen Fehlalarm-Meldungen belästigt werden.

Einmal aktiviert, übernimmt TBFILE vom Speicher aus die ständige Überwachung und gibt, sowie eine suspekte Manipulation entdeckt wird, in dem hierfür eingeblendeten Melde-Fenster eine entsprechende Meldung aus.

Folgende Meldungen sind möglich:

- **„Attempt to modify startup-code of <filename> ...."** – Versuch, die Startroutine der Datei <Dateiname> zu verändern.

Ein solches Unterfangen läßt zweifelsfrei auf einen Virus schließen, denn kein Programm speichert veränderbare Programmteile, wie das Konfigurations-Setup, in der Startroutine!

- **„Attempt to add some code to program file <filename> ..."** Versuch, den Programmcode zu erweitern.

Vorsicht! Es könnte ein Virus sein, der sich an den Code des Wirtsprogramms anzuhängen versucht!

- **„Attempt to modify <filename>, using obsolete FCB-functions ..."** – Versuch, die Datei durch unzulässige Datei-Kontroll-Blockfunktionen zu verändern.
- **„Attempt to rename <filename> to <filename> ..."** – Versuch, die Datei umzubenennen.

Achtung! TBFILE kontrolliert nur ausführbare .EXE- und .COM-Dateien. Der Versuch, die Erweiterung einer Programmdatei umzubenennen, ist im höchsten Maße verdächtig!

- **„Attempt to set the seconds part of <filename>'s time-stamp to an invalid value ..."** – Versuch, den (versteckten!) Sekundenwert beim Zeiteintrag durch einen ungültigen Wert zu ersetzen.
- **„Attempt to remove the read-only attribute for <file-name>..."** – Versuch, das Nur-Lese-Attribut der Datei zu entfernen.

TBDISK

Eine ganze Reihe von Viren haben es speziell auf die Festplatte abgesehen und trachten danach, diese neu zu formatieren oder Sektoren zu vertauschen oder was sonst an bösartigen Aktivitäten noch möglich ist.

TBDISK hat die Aufgabe, die Festplatte zu überwachen, und richtet sich zu diesem Zwecke resident im Speicher ein. Permanent auf der Lauer, daß kein Virus eindringt oder eingeschleust werden kann, paßt TBDISK auf, daß kein Programm unter Umgehung von DOS direkt auf die Festplatte schreibt. Warum das?

Sowie nun ein direkter Schreibzugriff erfolgt, öffnet sich ein Fenster mit einer entsprechenden Meldung. Darauf müssen Sie entscheiden, ob dieser Zugriff abgebrochen oder fortgeführt werden soll. Antworten Sie auf die Frage *Cancel direct access?* mit *Nein,* so wird im Programm fortgefahren, und das betroffene Programm wird in der Anti-Viren-Datei mit einer entsprechenden Markierung versehen.

Eine besondere Art oder vielmehr Abart der gemeinen Computerviren ist darauf programmiert, Bootsektor-Viren auf die Festplatte einzuschleusen – die sogenannten **Dropper oder Schlepper.** Diese Viren-Schlepper sind nur sehr schwer zu identifizieren – eben, weil sie selbst keine Viren sind. TBDISK ist darauf ausgerichtet, auch diesen Eindringlingen das Handwerk zu legen. Dropper pflegen bei ihrem niederträchtigen Unterfangen direkt auf das BIOS zuzugreifen und das Betriebssystem zu umgehen. Im Unterschied zu Viren-Programmen greifen normale Programme in den allermeisten Fällen nicht direkt auf die Festplatte zu, sondern nutzen das Betriebssystem DOS. Doch es gibt Ausnahmen wie z. B. die unterschiedlichen Formatier- und Diagnose-Utilities.

Wie unterscheidet TBDISK, ob ein Programm legal oder illegal auf die Festplatte schreibt?

Um die entsprechende Unterscheidung treffen zu können, benötigt TBDISK wiederum die Aufzeichnungen in den vom Setup-Programm angelegten Anti-Viren-Dateien.

TBGARBLE

Das letzte Programm im Menü TBAV MONITOR ist ein Disketten-Verschlüsselungs-Programm, das vor allem bei Multi-User- und Netzwerkbetrieb interessant ist. **TBGARBLE** bietet die Möglichkeit, **Disketten zu verschlüsseln und zu entschlüsseln,** um unerwünschtem Diskettenaustausch auf diese Weise einen Riegel vorzuschieben.

Das Verschlüsseln und Entschlüsseln der Disketten läuft ab, ohne daß Sie selbst etwas dazu tun, und ohne daß Daten dazu konvertiert werden müssen! Wie wird das bewerkstelligt? Ganz einfach: Beim Formatieren. Wenn TBGARBLE aktiv ist, so werden automatisch alle Daten beim Schreiben auf die Diskette verschlüsselt und beim Lesen entschlüsselt.

Bei der Verschlüsselung wird bei allen nichtregistrierten Shareware-Versionen der Thunderbyte-Utilities derselbe Schlüssel verwendet. Registrierte Anwender dagegen erhalten die erforderlichen Informationen und Instruktionen, um eine eigene Schlüsseldatei anzulegen. Als registrierter Anwender sollten Sie nicht vergessen, sich von Ihrem Key-File eine Backup-Kopie anzulegen!

Registrierte Anwender erhalten die erforderlichen Informationen und Instruktionen, um eine eigene Schlüsseldatei anzulegen, die den Namen und die Lizenznummer und eben das von Thunderbyte für jeden Anwender eigens vergebene Schlüsselwort enthält. Ohne Kenntnis dieses Schlüsselworts ist es unmöglich, auf diese Datei zuzugreifen und verschlüsselte Dateien zu entschlüsseln.

Heftdiskette defekt?

In diesem Fall verwenden Sie den Reklamationsschein auf dieser Seite. Bitte deutlich lesbar ausfüllen und zusammen mit einem ausreichend frankierten Rückumschlag (bis 100 g: DM 3,–) an die DOS-TREND-Redaktion, Am Kalischacht 4, 79426 Buggingen senden.

Adresse

Vorname

Nachname

Straße

PLZ / Ort

Reklamationsschein

Hier bitte das Etikett Ihrer Programmdiskette aufkleben – ganz oder teilweise. Wichtig: die Seriennummer muß lesbar sein! Wir vertrauen Ihren Angaben – bitte Diskette nicht mitsenden!

meine Telefonnr.:

Etikett der Diskette

Bitte schreiben Sie deutlich Ihre Absenderadresse in das Adreßfeld!

Disk-Tausch gratis

Seit der Ausgabe EXTRA 1 bieten wir Ihnen die Möglichkeit, kostenlos – gegen Rückporto und Umschlag – die Heftdiskette im 3½-Zoll-Format zu bestellen. Nehmen Sie bitte einen ausreichend frankierten Briefumschlag (bis 100 g: DM 3,–), versehen Sie ihn mit Ihrer eigenen Anschrift und senden Sie ihn an die

DOS-TREND-Redaktion · Stichwort: „Diskettentausch 3½-Zoll-Format"
Am Kalischacht 4 · 79426 Buggingen

Die deutsche Vollversion

Die vorliegende Sharewareversion der Thunderbyte Anti-Viren-Utilities ist voll funktionsfähig und kann uneingeschränkt und ausgiebig getestet werden.

Doch verwechseln Sie Shareware bitte nicht mit Freeware! Wenn Sie das Programmpaket getestet und sich davon überzeugt haben, daß es zum gegenwärtigen Zeitpunkt kein besseres und zuverlässigeres Schutz- und Präventiv-Programm gibt, dann lassen Sie sich registrieren.

Profitieren Sie von den vielfältigen Vorteilen, die der Erwerb der Vollversion und die Registrierung bieten:

Hotline-Support

• Registrierten Anwendern steht jederzeit der Thunderbyte Hotline-Support zur Verfügung. Kompetente Unterstützung und Beratung aus erster Hand – im Ernstfall keine Alternative!

Analyse-Service

• Virenverdächtige Programme können von registrierten Anwendern zur Überprüfung und Analysierung an die Spezial-Labors von Thunderbyte gesandt werden.

Zusatzoptionen

• Die Vollversion enthält einige zusätzliche Programmoptionen, die in der Shareware nicht verfügbar sind, wie etwa Dateiverschlüsselungs-Optionen.

Spezielles Key-File

• Mit dem Erwerb der Vollversion erhalten Sie ein spezielles eigenes KEY-File, das Ihnen einen zusätzlichen Schutz bietet.

Deutsche Fassung

• Die Vollversion enthält die Thunderbyte Anti-Viren-Utilities in deutscher Fassung – kein mühseliges Fachwörterbuchwälzen mehr.

Deutsches Handbuch

• In der Vollversion erhalten Sie das vollständige Handbuch (über 200 Seiten!) in deutscher Übersetzung auf der Diskette: schnelles und müheloses Auffinden aller wichtigen Hintergrund-Informationen – interessant sowohl für Profis als auch für Einsteiger.

Deshalb:
Nutzen Sie die vielfältigen Vorteile der Vollversion und lassen Sie sich registrieren!

DOS TREND EXTRA

Redaktion: Dr. Marianne Steible (verantwortlich für den Inhalt)

Mitarbeiter: Berthold Hess

Heftdiskette: Pearl Agency, Buggingen (Zusammenstellung und Vervielfältigung)

Art Director, Layout: Jochen F. Uebel (textwerkstatt, Sulzburg)

Titel: ARTelier Lunke, Stuttgart

Verlag: TREND-Redaktion
Am Kalischacht 4, 79426 Buggingen
Tel.: (07631) 360-0, Fax: (07631) 360-444

Grossistenbetreuung: Uwe Klein,
Am Kalischacht 4, 79426 Buggingen
Tel.:(07631) 360-0
Fax:(07631) 360-444

Anzeigenleitung: Jürgen Kaupp
Am Kalischacht 4, 79426 Buggingen
Tel.:(07631)360-0, Fax:(07631)360-444

Erscheinungsweise: Bis zu 6 Ausgaben / Jahr

Verbreitete Auflage: 80 000 Ex.

Lithografie: Printshop Schimann GmbH, Karlskron

Druck: MARCO srl, Industrie Litografiche, Torino

Verkaufspreis: DM 8,50

Bankverbindung: Spar- und Kreditbank Bad Krozingen, BLZ 680 632 54, Kto. 15949.2

Bezugsmöglichkeiten: Bestellungen nehmen der Verlag und alle Buchhandlungen im In- und Ausland entgegen. Für unverlangt eingesandte Manuskripte und Datenträger sowie Fotos übernimmt der Verlag keine Haftung. Ebenfalls ausgeschlossen ist die Haftung für die Richtigkeit der Veröffentlichung, trotz jeweils sorgfältiger Prüfung durch die Redaktion. Die Rücksendung ist ausgeschlossen.

Das Urheberrecht für veröffentlichte Manuskripte liegt ausschließlich beim Verlag. Nachdruck, Vervielfältigung oder sonstige Verwertung von Beiträgen nur mit schriftlicher Genehmigung des Verlages.

Namentlich gekennzeichnete Artikel geben nicht in jedem Fall die Meinung der Redaktion wieder. Sämtliche Veröffentlichungen im DOS-TREND-Sonderheft erfolgen ohne Berücksichtigungen eines eventuellen Patentschutzes, auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.

Die jeweils gültige Anzeigen-Preisliste ist zu erfragen.

LIEFERN SIE MIR GEGEN (Versandkosten in Klammern)

- ☐ **Bankeinzug** (+ DM 4,90) Bitte Bankverbindung angeben
- ☐ **Scheck liegt bei** (+ DM 5,90)
- ☐ **Nachnahme** (+ DM 7,90)
- ☐ **Rechnung** (+ DM 9,90) Nur Großfirmen/öffentliche Institutionen mit offizieller Bestellung)

Hiermit bestelle ich: (Passend für Fensterbriefumschläge)

____ **Vollversion der Thunderbyte Anti-Viren-Utilities** (Best.-Nr. VD2828) ..... **DM 124,80**

(abzüglich Gutschrift von DM 8,50 für Shareware, zuzüglich Versandkostenanteil)

Absender

Vorname ____ Nachname ____
Straße/Hausnummer ____
Land / neue PLZ ____ Ort ____
BLZ ____ Konto ____
Name der Bank ____
Datum ____ Unterschrift ____

PEARL
Agency Allgemeine Vermittlungsges. mbH
Am Kalischacht 4
D-79426 Buggingen

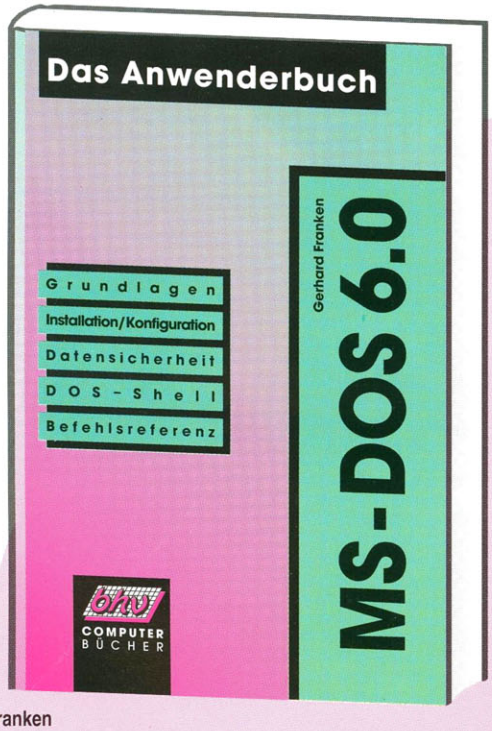
Bestellannahme: (0 76 31) 360-200 **MO-FR** 8-20 Uhr **SA+SO** 16-20 Uhr
Telefonzentrale: (0 76 31) 360-0 **Telefax:** (0 76 31) 360-444
BTX *pearl# **Mailbox** (0 76 31) 1 20 21

Österreich Steyrer Str. 40 · A-4540 Bad Hall **Tel** (07258) 5333 · **Fax** (07258) 5315 Preise: **ÖS = DM x 8**

Auf Bestellungen unter einem Auftragswert von DM 30,– erheben wir einen Mindermengenzuschlag von DM 4,–.

DIE BÜCHER ZU MS-DOS 6.0

AKTUELL IM AUGUST / SEPTEMBER



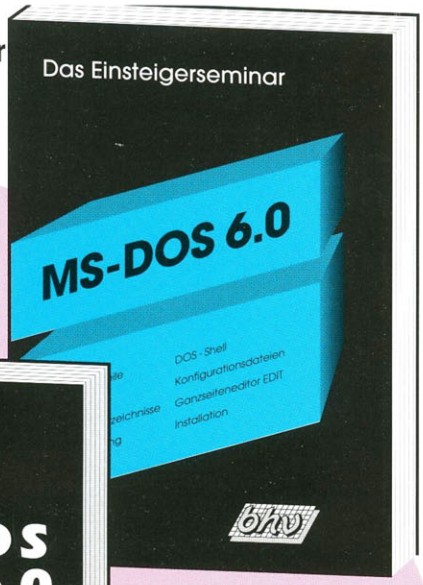
Gerhard Franken

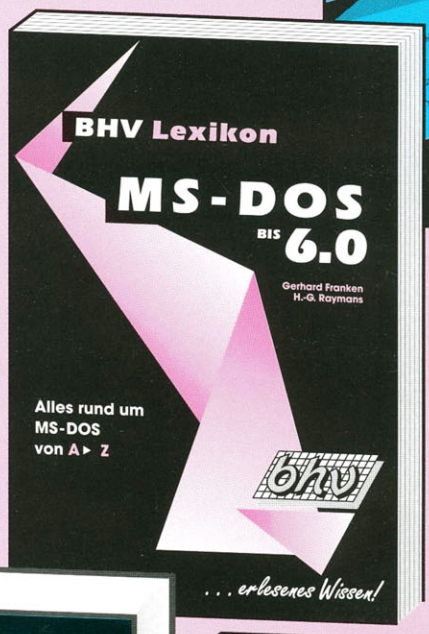
Das Einsteigerseminar MS-DOS 6.0

ISBN 3-89360-704-8
224 Seiten, broschiert

19,80 DM

Dieses Buch ist bewußt kompakt gehalten und beschränkt sich auf die für die Praxis wesentlichen Programmfunktionen. In kurzen Lernabschnitten wird, unterstützt von vielen Übungs- und Arbeitsaufgaben, der Einstieg in das Betriebssystem MS-DOS 6.0 vermittelt.





H.-G. Raymans / T. Schlabach

BHV Lexikon MS-DOS bis 6.0

ISBN 3-89360-709-9
224 Seiten, broschiert

19,80 DM

Alles über MS-DOS von A -Z in über 800 Stichwörtern:Tips & Tricks, Installation, Speicherverwaltung, Konfiguration, Stapeldateien, DOS-Editoren, Datenschutz, Laufwerke, Verzeichnisse etc.

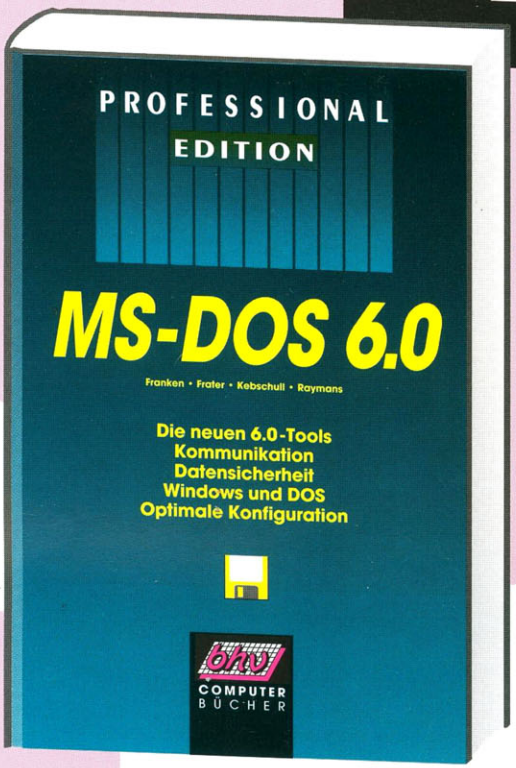
Gerhard Franken

Das Anwenderbuch MS-DOS 6.0

ISBN 3-89360-036-1
640 Seiten, gebunden

39,00 DM

In diesem Anwenderbuch bereitet Autor Gerhard Franken sein Wissen für Sie in wirklich verständlicher und kompetenter Weise auf, so daß es sowohl für frischgebackene Einsteiger als auch für fortgeschrittene Anwender den idealen DOS-Ratgeber darstellt.



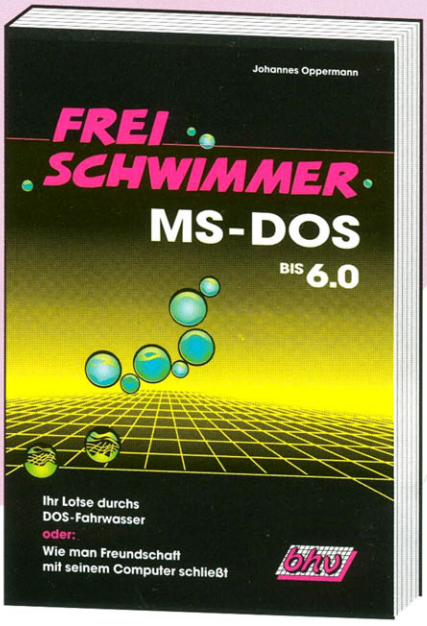
Franken/Frater/Kebschull/Raymans

Professional Edition MS-DOS 6.0

ISBN 3-89360-306-9
736 Seiten, gebunden, mit Diskette, Ausklappseiten

59,00 DM

Unser Standardwerk behandelt sämtliche DOS-Versionen. In seinen verschiedenen Teilen werden u. a. die Arbeitsumgebung und die Werkzeuge von DOS (EDIT, DEBUG und DOSKEY), Batch- und Konfigurationsdateien, Speichermanagement unter Berücksichtigung von Windows, Multitasking, File-Sharing, die neuen 6.0 Tools und Virenbekämpfung ausführlich erörtert. Sie finden wertvolle Tips zur Optimierung Ihres Systems sowie undokumentierte DOS-Befehle.



Johannes Oppermann

Freischwimmer MS-DOS bis 6.0

ISBN 3-89360-045-0
344 Seiten, broschiert

24,80 DM

Was immer Sie gehört und gelesen haben – an MS-DOS kommen Sie als PC-Anwender nicht vorbei. Aber glauben Sie ja nicht, DOS sei zu schwer für Sie! In diesem Buch werden Sie sehen, wie einfach es ist, mit seinem Computer Freundschaft zu schließen. Sie erhalten hier eine einfühlsame Einführung in die grundlegenden Elemente von DOS, ganz gleich, welche Versionsnummer Ihr DOS hat.

BHV Verlags GmbH, Postfach 30 01 62, 41342 Korschenbroich
Tel.: 0 21 82 / 40 63-65, Fax: 0 21 82 / 5 09 15, **BTX: ⋆ BHV#**
Österreich: Christian Konrad GmbH, Herrgottschnitzergasse 8, A-2344 Maria Enzersdorf, Tel.: 0 22 36 / 27 371, Fax: 0 22 36 / 27 372
Schweiz: Freihofer AG, Weinbergstraße 109, CH-8033 Zürich, Tel.: 01 / 362 92 97, Fax: 01 / 363 40 57

Ein Konzept setzt sich durch!

Anforderungsschein

Bitte senden Sie mir den BHV-Gesamtkatalog
BHV Verlags GmbH, Postfach 30 01 62, 41342 Korschenbroich
Tel.: 0 21 82 / 40 63-65, Fax: 0 21 82 / 5 09 15, **BTX: ⋆BHV #**

Name
Straße
PLZ / Ort

DT8/93D

Thunderbyte Utilities

Achtung: TBAV-Utilities V 6.04
Neueste Version erst nach Redaktionsschluß! Die Aktualität eines Anti-Viren-Programmes ist absolut wichtig! Auf der Heftdiskette befindet sich daher die allerneuste Fassung!

Achtung: Rund 2500 bekannte Computerviren treiben zur Zeit ihr Unwesen und zerstören tagtäglich wertvolle Datenbestände!

Kein PC-Anwender sollte sich vorschnell in Sicherheit wähnen – selbst dann nicht, wenn er ein Antiviren-Programm auf seinem Rechner installiert hat. Denn bei der Bekämpfung von Computerviren haben die Anti-Viren-Programmierer einige Mühe, angemessene Schutz- und Abwehrmaßnahmen gegen die immer wieder neuen und immer raffinierteren Eindringlinge ins Feld zu führen.

Der niederländischen Firma **ESaSS** ist mit den **Thunderbyte-Utilities** ein Rundumschutz gelungen, der Computer-Anwendern ein bislang nicht erreichtes Maß an Sicherheit **auch vor unbekannten** Viren bietet. Thunderbyte entdeckt Computerviren, bevor sie virulent sind!

Das Thunderbyte-Konzept basiert auf jahrelangen intensiven Forschungsaktivitäten und auf den modernsten Verfahren der Virenerkennung und Virenabwehr. Die einzelnen Module im Thunderbyte Anti-Viren-Paket umfassen **alle Stufen der Virenbekämpfung** von der **Diagnose** bis zur **Immunisierung** und **Prävention** und realisieren in ihrem Zusammenwirken ein **umfassendes und lückenloses Sicherheitskonzept.**

Inhalt der Heftdiskette:

TBSCAN: Dieser Virenscanner beschränkt sich nicht auf bloßes Signaturen-Scannen, sondern analysiert und interpretiert interne Programmbefehle. Dank dieses **exklusiv** von Thunderbyte entwickelten **heuristischen Verfahrens** können **auch unbekannte und noch nicht identifizierte Viren** aufgespürt werden.

TBCHECK: Speicherresident installiert, kontrolliert dieses Prüfsummenprogramm Programmdateien auf ihre Integrität und **meldet jede Veränderung und jede unerlaubte Manipulation.**

TBUTIL: Mit diesem nützlichen Utility können Sie ein **Backup des Bootsektors, der Partitions-Tabelle und der CMOS-Einstellungen anlegen.** Bei einer Infizierung mit Bootsektor-Viren lassen sich die wichtigsten Systemdaten **rekonstruieren.**

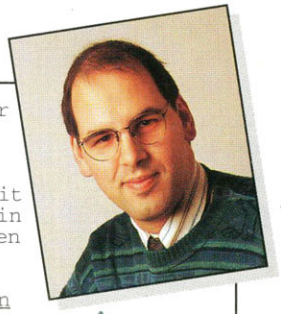
TBCLEAN: Das „Desinfektionsprogramm" **entfernt bekannte und unbekannte Viren und stellt beschädigte Dateien wieder her.**

TBMEM: Mit Argusaugen überwacht dieses speicherresidente Kontrollprogramm den Speicher und **verwehrt ungebetenen Eindringlingen den Zutritt.** Kein Programm vermag sich mehr unerlaubt in Ihrem Arbeitsspeicher festzusetzen!

TBFILE: Dateiviren haben keine Chance! Dieser **Dateiwächter** sorgt dafür, daß **kein Programm ein anderes Programm infiziert!**

TBDISK: Das residente Überwachungsprogramm **kontrolliert die Festplatte** und läßt keinen unerlaubten Schreibzugriff zu.

Thunderbyte bietet ein komplettes Instrumentarium zum Schutz und zur Abwehr von Computerviren – einen Rundumschutz, auf den kein PC-Besitzer verzichten kann!



Sehr geehrte TBAV-Anwender

Als Technischer Direktor von ESaSS freue ich mich, Ihnen in Zusammenarbeit mit der DOS-TREND-Redaktion ein Anti-Viren-Paket vorstellen zu dürfen, das den Herausforderungen selbst noch nicht bekannter Viren ganz und gar gewachsen ist. Ob Dropper, Datei- Stealth- oder Bootsektor-Viren - selbst polymorphe Viren und die gefürchteten „Mutation Engines" sind für die ThunderByte Anti-Viren-Utilities kein Problem. Dafür stehe ich mit meinem Namen.

Frans Veldmann
Verantwortlich für die Entwicklung der ThunderByte Anti-Viren-Utilities bei ESaSS / Niederlande